Doc ID: 6592458

~~TOP SECRET~~

KROEGER'S [illegible]

ARMED FORCES SECURITY AGENCY

DF 240-A

19/51/~~TOPSEC~~/AFSA-14

Copy No. 27

From: AFSA-14

To: _____

Approved for Release by NSA on 09-12-2017, FOIA Case #67677

~~TOP SECRET~~

Doc ID: 6592458

DF 240-A 19/51/~~TOPSEC~~/AFSA-14

CHARACTERISTICS, ANALYSIS AND SECURITY OF CRYPTOGRAPHIC SYSTEMS

TABLE OF CONTENTS

1. Shortly after Hitler's assumption of power Hermann Goering was sold the idea of setting up a new, comprehensive intelligence agency which would supply the Party and in particular Goering himself with all possible secret information. The new agency bore the innocent name "Das Forschungsamt des Reichsluftministeriums" (The Research Office of the German Air Ministry) but was really Goering's private affair. He secured ample funds, the FA, as it was called, soon had new buildings and the most up-to-date equipment. Some of the leading spirits had been discontented members of the Cipher Bureau of the Armed Forces, a few were capable cryptanalysts. It covered all fields of communication, mail, telephone, cable, broadcasts and radio; it spied on all other branches of the government and the results of its work were used to induce Hitler to purge a number of men who were obnoxious to Goering. Little was known in the West about the existence of this agency until TICOM Teams began to pick up information after the surrender. Even then most of the information came from men in other agencies, some of whom were doubtless prejudiced against the FA. Estimates of the value of the FA were conflicting.

2. Eventually an opportunity came to get information from some of the members of the Forschungsamt itself. Those who originally agreed to write accounts of the organization and its work later declined to do so, but finally arrangments were made for a group of three men to do some homework. A list of questions was submitted.

3. Dr. Kroeger, the leader of this small group, has chosen to answer some of the questions separately but to combine the answers to others into a treatise "SYSTEMATIK, ANALYSE UND SICHERHEIT DER GEHEIMSCHRIFTEN". The present paper is offered to show the scope of the project and a sample section (III A 1 a) was submitted to give an idea of the treatment. This section has been translated and is being issued simultaneously as DF 240-B. Answers to the other questions will be translated and issued under the general short title DF 241. It is hoped that the two series, DF 240 and DF 241, will add materially to our knowledge of the Forschungsamt and its work.

4. Dr. Kroeger is willing to be guided in his work by comments and suggestions, provided they reach him in time. Any comments should, therefore, be forwarded to AFSA-14 promptly.

April 1951 35 copies
Translated: R.W.P. 6 pages
Distribution: Normal

oc ID: 6592458

DF 240-A

TABLE OF CONTENTS
to the
TREATISE

CHARACTERISTICS, ANALYSIS AND SECURITY OF CRYPTOGRAPHIC SYSTEMS

Introduction

I. GRUNDVERFAHREN
General systems

A. Ersatzverfahren
Substitution Systems

1) Einfacher Buchstabencäsar
Simple monoalphabetic substitution

a) alphabetisch
with standard alphabets

b) systematisch
with systematically mixed alphabets

c) reziprok
with reciprocal alphabets

d) unsystematisch
with random alphabet

2) Einfacher Zahlencäsar
Simple numerical substitution

3) Mehrfach belegter Zahlencäsar einschliesslich 2 Z Cr 100
Dinome substitution with variants, including all 100 dinomes (?)

4) Deutscher Paarcäsar
German digraphic substitution

5) Englischer Paarcäsar
Playfair cipher

6) Wechselstelliger Zahlencäsar
Monome-dinome substitution

7) Spaltencäsar
Periodic polyalphabetic substitution

a) Tritheim
Tritheim [Viginere table]

b) unsystematisch
random unrelated sequences

c) Kommunistenverfahren
Communist systems

d) Buchverschlüsselung
Encipherment by means of a key book.

DF 240 A

8) Springcäsar
interrupted periodic polyalphabetic substitution

9) Systematik bei Spalten- und Springcäsaren
Systematic features of polyalphabetic substitutions with regular or interrupted period (?)

a) kurzer Schieber
short slide

b) langer Schieber
long slide

10) Spaltencäsar mit Wahlverzifferung
Periodic substitution with optional keyword (?)

11) Codes
Codes

a) alphabetische und systematische codes
one part and caption codes

b) unsystematische und wechselstellige codes
two part codes and codes with groups of varying length

c) Mehrfachbelegung von codes
Use of variants

B. Versatzverfahren
Transposition systems

1) Umstellung
Shifting of group elements (?)

2) Drehraster, Schieberaster
Revolving grille, sliding grille

3) Würfel
Matrix (box) transposition

a) einfacher Würfel
simple (rectangular) matrix

b) besondere Würfelformen
special matrix forms

c) Schlüsselwörter und Schlüsselzahlen
Key words and numerical keys

II. KOMBINIERTE BEZW. "ÜBERSCHLÜSSELTE" VERFAHREN
Combined or Superenciphered Systems

A. "Überschlüsselungen"
Superencipherments

1) Tauschtafelüberschlüsselung
reencipherment by substitution table

a) einstellige Tauschtafeln
one place substitution tables

b) mehrstellige Tauschtafeln
multi-place substitution tables

c) Perioden
periods

DF 240 A

2) Überschlüsselungszahlen im Additionsverfahren
Superencipherment by additive

a) relative Codes
relative codes

b) beschränkte Überschlüsselungszahlen
finite additive sequence

c) Ü Z[= Überschlüsselungszahlen]- Tafeln
Additive tables

d) Ü Z - unendlich
Additive sequence - non-repeating

e) russische Ü Z aus Schlüsselzahlen entwickelt
Russian additive derived from key numbers

3) Überschlüsselungszahlen im Tauschtafelverfahren
Superencipherment numbers in substitution table systems

B. Kombinierte Verfahren
Combined systems

1) Doppelwürfel
Double transposition

2) Würfel mit Raster
Transposition matrix with grille

3) Cäsar und Codes mit Umstellung
Substitution and codes with shifting of elements (?)

4) Cäsar and Codes mit Würfel
Substitution and codes with transposition

5) Tauschtafel mit Umstellung
Substitution table with shifting (?)

6) Überschlüsselungszahl mit Umstellung
Reencipherment number with shifting (?)

III. CHIFFRIERMASCHINEN
Cipher Machines

A. Deutsche Typen
German types

1) Enigma-Maschinen
Enigma machines

a) Type K
" "

b) Type G
" "

c) Heeres-Enigma
Army Enigma

DF 240 A

2) Siemens-Geheimfernschreibmaschinen
Siemens Secret Teleprinter

a) SMF 52 Typ AB
b) SMF 52 Typ C
c) SMF 52 Typ D und E

3) Heereszusatzgerät
Army supplemental (cipher) device

B. Andere Typen
Other types

1) Japanische Maschine
Japanese Machine

2) Hagelin-Maschinen
Hagelin machines

3) Russiche Mehrkabel-Funkmaschinen
Russian multi-channel radio equipment

4) Englische Maschine
English machine

C. Kenngruppenbedeutung bei Maschinenverfahren
Significance of indicator groups with machine systems

IV. ALLGEMEINE BEMERKUNGEN UND ERGÄNZUNGEN zur
General and suplementary remarks on

A. Systematik der Geheimschriffen
Systematic character of cryptographic systems

B. Analyse von Geheimschriften
Analysis of cryptographic systems

C. Sicherheit von Geheimschrfiten gegen unbefugte Entzifferung von dritter Seite.
Security of cryptographic systems against unauthorized decryption by third parties.

Doc ID: 6592459

ARMED FORCES SECURITY AGENCY

DF 240-B

20/51/~~TOPSEC~~/AFSA-14

Copy No. 2

From: AFSA-14

To: AFSA-141

07Sep/2012
2 Sep82

Do NOT Destroy Return to the NSA Technical Library when no longer needed
Copy No. 2

Approved for Release by NSA on 09-12-2017, FOIA Case #67677

Doc ID: 6592459

DF 240-B 20/51/~~TOPSEC~~-AFSA-14

CHARACTERISTICS, ANALYSIS AND SECURITY OF CRYPTOGRAPHIC SYSTEMS

Analysis of the Enigma Cipher Machine Type K
(III. A 1 a)

1. Attached is an Armed Forces Security Agency translation of a sample section of the treatise being written by Dr. Kroeger, formerly with Goering's cryptologic agency the "Forschungsamt". The German title of the treatise as a whole is "SYSTEMATIK, ANALYSE UND SICHERHEIT DER GEHEIMSCHRIFTEN", the title of this section is "ANALYSE DER CHIFFRIER-MASCHINE ENIGMA TYP K".

2. The section on the Enigma Type K was submitted as a sample, along with the proposed Table of Contents (see DF 240 A), with the suggestion that any comments be forwarded to the author in time for him to take them into account while composing the rest of the work. Comments should be sent promptly to AFSA-14.

3. At the same time answers were received to certain questions submitted to Dr. Kroeger and his associates; these are being issued as DF 241 A. Answers to other questions and additional installments of the major work are expected and will be issued as received. The two series, DF 240 and DF 241 will, it is hoped, add materially to our knowledge of the Forschungsamt and its work.

Translated: R.W.P. 35 copies
Edited: R.E.C.
April 1951 23 pages
Distribution: Normal

Doc ID: 6592459

CHARACTERISTICS, ANALYSIS AND SECURITY OF CRYPTOGRAPHIC SYSTEMS

Analysis of the Enigma Cipher Machine Type K

(III. A 1 a)

a. Analysis of the Enigma Cipher Machine Type K.

Part 1: Development of the regularities of the cipher text which are due to the construction of the Type K Enigma.

Part 2: Possibilities of solution based on these regularities.

Possibility A

Possibility B

Part 3: Estimate of the security of the Enigma Cipher Machine

Appendix III A 1 a, sheets 1 to 8.

Part 1

The construction and functioning of the Enigma Type K is assumed to be known. It is shown schematically as a paper device in Appendix III A 1 a, sheet 1; by the aid of this paper device any cipher text can be produced in the same manner as with the machine itself, assuming the wheel wirings agree.

In Appendix III A 1 a, sheet 1 *; the column of letters at the right corresponds to a fixed disk in the original machine which lies to the right of the right hand movable wheel. In the machine this disk is connected both with the key board and with the illuminated letters in the sequence of the letters in this column, which therefore is designated hereafter as the entry wheel alphabet **.

---

* Editor's note: It has been felt advisable to include, in addition to the original analogue which has been constructed in a manner which may be unfamiliar to some, another analogue which is the cryptographic equivalent of the original and has been made in accord with those used in our own courses of instruction; this appears as sheet 1a, and follows sheet 1. This analogue may be used throughout in place of the original.

** Editor's note: In our own terminology, the "endplate sequence."

Doc ID: 6592459

The paper strips I, II and III represent the wheels themselves which may stand in the positions A, B, and C corresponding to the wheel order selected. The outer sequences of numbers running from 1 to 26 at the right and left of each strip correspond to the 26 points of entry and exit on each wheel. We have designated as Point 1 that point on each wheel at which the letter ring has been set. The inner sequences of numbers show the wiring within the wheels and the numbers of the inner sequences indicate the point on the opposite face of the wheel with which the particular point of entry or exit is connected.* The two columns of numbers standing on the left side of the paper device correspond to the reversing wheel or mirror wheel in a specific position and with a given wiring. The sequences of letters in the middle of the paper strips represent the setting rings on the wheel in a specific position. The lines between the letters m and n on Wheel I, f and g on Wheel II, y and z on Wheel III are intended to indicate the notches on the setting rings into which the transport lever** (indicated in the paper device by an arrow) engages at the appropriate position and thus causes the stepping of the middle wheel or of the left wheel. The hatched squares shown in the bottom row (on a level with q of the entry alphabet) are intended to represent the windows in which the window setting of the wheel is visible.

With this paper device, with the arbitrarily assigned wheel order I III II, the inner ring setting v for Wheel I, l for Wheel II and h for Wheel III and the external window setting n c f for the three wheels, all the cipher values for the plain text letters of the sequence of the entry wheel have been developed in 26 successive positions of the right wheel and are shown in Appendix III A 1 a, sheet 2. In so doing the first 21 of the resulting substitution alphabets have been so separated from the

* Editor's note: It is not essential that both "outer" and "inner" sequences should appear on the strips, as in the original analogue. The strips used on sheet 1a contain only one sequence on each side, yet are the equivalents of the original ones.

** Editor's note: In our own terminology, the "trip lug."

last five by a vertical stroke, because at this point the middle wheel made a step. Hence at this point the wheel complex - reversing wheel, Wheel I and Wheel III, which really forms a reversing mirror - is changed.

The following presentation of the regularities of the cipher text of the Enigma Cipher Machine Type K rests upon the basic idea that the reversing wheel, the left wheel and the middle wheel form a constant during the encipherment of 26 letters which lie between the steps of the middle wheel. Consequently we have underlying the encipherment of 26 successive cipher letters in each case merely:

1. The wheel wiring of the right wheel and
2. The reversing mirror formed by the reversing wheel, the left wheel and the middle wheel.

Our task in the following is therefore to develop the cipher texts of Appendix III A 1 a, sheet 2, in such fashion that the regularities inherent in the wiring of the right wheel and in the reversing mirror can be recognized.

For this purpose the substitution alphabets of Appendix III A 1 a, sheet 2, have been converted in Appendix III A 1 a, sheet 3, into numerical values in such fashion that the letters q to m have been transformed into the entrance wheel values 21 to 20 which are valid with the initial position f for the right wheel.

In Appendix III A 1 a, sheet 4, numbers have been added to the numerical values in Appendix III A 1 a, sheet 3, as follows: 1 to the values of the second substitution alphabet (i.e. to the second vertical column of numbers), 2 to those of alphabet 3, 3 to those of alphabet 4 etc., whereby all the cipher letters of Appendix 3 A 1 a, sheet 1*, have been converted into the entry values of this wheel which are valid in the wheel position of the right wheel at the moment. Through this transformation we have succeeded in bringing the substitution alphabet values of Appendix III A 1 a, sheet 1**, to a uniform denominator which is independent of the movement of the right wheel.

* Editor's note: Should read "sheet 2".

** Editor's note: Should read "sheet 3".

Doc ID: 6592459

In Appendix III A 1 a, sheet 4, the numerical substitution alphabet values standing in the diagonals running down from left to right have been formed in each case by the same wheel wiring leading from the entry wheel alphabet to the reversing mirror.

In the next Appendix III A 1 a, sheet 5, these diagonals have been taken out and arranged horizontally. A closer study shows that these sequences are similar to one another in their structure, as a comparison of diagonal 7 with diagonal 6 reveals. Here the structurally similar make-up of each series with any other series appears with the displacement of one value to the right in each case. The values found in each of these diagonal sequences have the same wheel wiring on their path from the entry alphabet to the reversing mirror which lies between the middle and right wheel and hence use in succession all mirror wirings of the reversing mirror corresponding to the stepping of the right wheel. The structural similarity of the diagonal series with one another is therefore only a reflection of the reversing mirror which is valid for the right wheel.

To further clarify this fact we have presented in Appendix III a 1 a, sheet 6:

1. The reversing mirror valid for the right wheel with the window setting n c f, as it is formed by the wheel complex: reversing wheel, Wheel I and Wheel III*;
2. The same reversing mirror expressed in difference values between the contact points;
3. Two different diagonal sequences from Appendix III A 1 a, sheet 5, at an elevation** corresponding to the reversing mirror.

---

* Editor's note: In the illustration cited, the number "1" is used to designate the contact point which is located directly "beside" the window at the right-hand side of wheel III; number "2" designates the point just above "1", "3", the point above "2", etc.

** Editor's note: That is, the sequences have been aligned in such a manner that corresponding points of the isomorphic pattern of each are adjacent or on the same horizontal line.

Doc ID: 6592459

The structural similiarity of the diagonal sequences to the reversing mirror expressed in difference values thus become quite evident.

Now if all diagonal series are arranged according to their structural similarity to the reversing mirror, as has been done in Appendix III A 1 a, sheet 7, and in Appendix III A 1 a, Sheet 8, (in this case with a displacement degree 1), then it is clear from Appendix III A 1 a, Sheet 8, that with this arrangement not only the vertical columns of numbers but also the number sequences of the diagonal series represent nothing other than the wheel wiring sequence of the right wheel, as it is found in the left inner column of wheel II in Appendix III A 1 a, sheet 1*.

Thus it is proven that by converting the plain text and cipher text letters into the corresponding numerical values of the entrance wheel series the wheel wiring of the Enigma Type K can be reconstructed.

Part 2

On the basis of the regularities shown in Part 1 we find the following possibilities of solution for the Enigma Cipher Machine Type K:

Possibility A. We assume the knowledge of three successive substitution alphabets, which have been obtained by solving several messages in the same key or in some other way.

These alphabets are converted into numerical values in the manner described in Part 1 and are entered on strips corresponding to the rows of Appendix III A 1 a, sheet 8. As an example we shall use the first three alphabets after the stepping of the middle wheel from the example in Part 1, i.e. alphabets 16 to 18 of Appendix III A 1 a, sheet 4, as they appear in Appendix III A 1 a, sheet 8; then we should have the following strips:

(1)	20	13	24	(10)	15	4	5	(19)	13	6	25
(2)	8	9	8	(11)	18	23	4	(20)	1	3	6
(3)	9	20	14	(12)	22	15	13	(21)	7	8	22
(4)	6	10	11	(13)	19	1	12	(22)	12	18	21
(5)	14	25	10	(14)	5	24	3	(23)	26	11	7
(6)	4	19	20	(15)	10	12	16	(24)	16	14	1
(7)	21	17	23	(16)	24	26	15	(25)	17	5	19
(8)	2	21	2	(17)	25	7	18	(26)	23	16	9
(9)	3	2	26	(18)	11	22	17				

* Editor's note: in the analogue on sheet 1a, the left-hand sequence of wheel II.

Doc ID: 6592459

Starting with any desired strip the other strips are associated ["linked"] one after the other to this initial strip, until from the conclusions drawn from the comparison it is determined whether the sequence of strips or of wheel wirings chosen is correct or not. Hence we shall assume first that strip (18) follows the initial strip (17):

(17) 25 7 18

(18) 11 22 18

The columns 7 11 and 18 22 which result signify, corresponding to the regularities demonstrated in Part 1, that, with an assumed wheel wiring sequence* 17 18, the sequences 7 11 and 18 22 result. If the strips corresponding to these wheel sequences are placed one beneath the other and the resulting deductions are made, we get the following:

1. (7) 21 17 23 (18) 11 22 17

(11) 18 23 4 (22) 12 18 21

Since the new sequence 23 23 would result and this is impossible, we have shown that the assumed sequence 17 18 was false.

Now the next assumption is made, that strip (17) is followed by strip (19). This yields the following:

---

* Editor's note: in the analogue on sheet 1a, the left-hand sequence.

1.) (17) 25 7 18
(19) 13 6 25

2.) (7) 21 17 23
(13) 19 1 12

3.) (23) 25 11 7
(1) 20 13 24

4.) (11) 18 23 4
(20) 1 3 6

5.) (4) 6 10 11
(3) 9 20 14

6.) (10) 15 4 5
(9) 3 2 26

7.) (5) 14 25 10
(2) 8 9 8

8.) (25) 17 5 19
(8) 2 21 2

9.) (19) 13 6 25
(21) 7 8 22

10.) (6) 4 19 20
(7) 21 17 23

11.) (20) 1 3 6
(17) 25 7 18

12.) (3) 9 20 14
(25) 17 5 19

13.) (14) 5 24 3
(5) 14 25 10

14.) (24) 16 14 1
(14) 5 24 3

(18) 11 22 17
(6) 4 19 20

(22) 12 18 21
(4) 6 10 11

(21) 7 8 22
(10) 15 4 5

(8) 2 21 2
(15) 10 12 16

(2) 8 9 8
(12) 22 15 13

(9) 3 2 26
(22) 12 18 21

(26) 23 16 9
(18) 11 22 17

(16) 24 26 15
(11) 18 23 4

(15) 10 12 16
(23) 26 11 7

(12) 22 15 13
(26) 23 16 9

(13) 19 1 12
(16) 24 26 15

(1) 20 13 24
(24) 16 14 1

From these fragments of the sequences we get the entire wiring of the right wheel as follows:

17 19 21 10 9 22 4 3 25 8 15 23 1 24 14 5 2 12

26 18 6 7 13 16 11 20 17.

This example proves that a minimum of three alphabets is sufficient for the reconstruction of a wheel wiring. (If the reversing mirror valid for the alphabets in question has two successive parallel wirings with the same interval, then a fourth alphabet is necessary in order to get a complete wheel sequence. Otherwise we get for the wheel wirings several fragments which are not contradictory within themselves and whose proper succession must be tested out with the available cipher text.

With the wheel wiring thus obtained for the right wheel we can only produce for the moment a wheel which will have the same effect, since we do not know from the wiring sequence itself to which points of the left wheel face it is to be associated. Therefore we must first make an arbitrary assumption which yields one of the twenty-six possible wheels which have the same effect. Which of these possible wheels represents the original wheel can only be determined after the reconstruction of the remaining wheels.

For the reconstruction of the middle wheel it is necessary to have three substitution alphabets available at an interval of 26 which will then be used for the reconstruction of the middle wheel in the manner shown above for the right wheel. These three requisite alphabets at an interval of 26 can be picked out of the available traffic rather easily. Here the procedure is to associate an assumed plain text (frequently used telegram beginnings or some other word 6 to 8 letters in length, the occurrence of which in the text can be assumed on the basis of the traffic or of contemporary events), to the cipher text in such fashion that for every possible position of plain text and cipher text with respect to one another it is possible with the already reconstructed wheel to produce the mirror connections which are yielded by the 26 possible initial positions of the wheel and the entry alphabet. If contradictions occur in the mirror connection that means that the assumed word cannot stand at the point under consideration with

Doc ID: 6592459

the assumed initial wheel setting. If no contradictions result, then the mirror connections obtained are used to form new plain text letters to the right and left of the appropriate position in this cipher text. If these can be expanded to make rational text and if the expansion yields confirmation of the mirror connections already obtained, then the correctness of the assumption is proven. After that it is merely a question of expanding the text beyond those points where the middle wheel has stepped, and on the basis of the connections of the new mirror thus obtained, to again expand the text until a plain text of some 60 to 80 letters is available which matches the cipher text. From this it is then possible, by producing the entry alphabet valid for the middle wheel, to form three alphabets at an interval of 26 which will make possible the reconstruction of a wheel with the same effect as the original middle wheel.

The third wheel can be constructed in like manner using a cipher text where the third wheel is in the middle position.

From the wheels thus formed, which have the same effect as the originals, the original wheels can be derived if the window setting of three already solved cipher texts is known where wheels I, II and III each appear once as the right wheel. From the window setting and the step of the middle wheel it can be determined which of the three wheels corresponds to the original wheel I, II or III. The right wheel face is then reduced to the original values by adding a number between 0 and 25. Then with the aid of the solved texts the left faces of the wheels are likewise brought into the original position by turning the wiring sequence to that position where the different wheels work together correctly.

Then if the key is sent in clear or the encipherment is known, every telegram can be read by setting up the inner and outer key just as it is read in the Cipher Bureau of the recipient.

If only the clear window setting is known, while the inner wheel setting is not known but is constant for a definite period of time, then the solution of one telegram by means of an assumed word is sufficient to enable one to read at once all other telegrams of the same period.

oc ID: 6592459

On the other hand if the inner and outer machine setting is not known, then for each individual message a point of attack must be worked out by means of an assumed plain text word, if one is to read the message. This work is very time consuming if it is done by hand; however the production of auxiliary devices working with electric relays is entirely within the bounds of possibility and with their aid a quick break into almost any telegram will be possible.

Possibility B. As known we assume a sort of compromised text, i.e. a cipher text which has been compromised because the plain text has become known. This compromised text, according to the position of the steps of the middle wheel, must have a minimum length of 52 to 65 letters. The substitution alphabet values obtained from the plain text and cipher text are converted into numerical values after the manner described in Part 1 and are entered on strips. In contrast to the strips 3 cells wide which were used for the reconstruction of the wheel wiring under possibility A in Part 2, the strips here have a width corresponding to the length of the text but only sporadic alphabet values appear on them. We now proceed to use these strips in much the same manner as was described in connection with possibility A in Part 2, with the sole difference that for each initial assumption regarding the wire sequence a second, third, fourth or even a fifth assumption must be made, before one can decide whether the assumptions made were correct or not. This would work out somewhat as follows:

If the first assumption of a wiring sequence (1) (2) gives no clue to another wiring sequence resulting therefrom, or if a resulting new wire sequence leads to no conclusion regarding the correctness of the first assumption, then it is expanded by a second assumption of a wiring sequence (1) (2) (3) or even (1) (2) (3) (4); in other words we continue making a new assumption until the possibility of this assumption is eliminated by resulting contradictions. The process is continued until by elimination of impossible wire sequences the correct sequence is found in connection with which no contradiction appears.

If the original window settings for the compromised text used are not known, this task is rendered more difficult by the fact that you cannot guess at what points in the text the middle wheel has moved. Hence it is necessary to assume a wheel stepping with the interval 26 successively at all possible positions, since alphabet values standing one beneath the other on two strips only lead to correct deductions regarding other wheel sequences when they have arisen with the same setting of the middle wheel.

To give an idea of the extent of this labor, it may be stated that the reconstruction of the first wheel in this manner can be performed in from 1 to 6 weeks with 5 to 6 workers, just depending on whether one hits on the original sequence early or late in the guessing process.

The reconstruction of the other two wheels can then be accomplished relatively quickly in the manner described under possibility A in Part 2.

Part 3

From the standpoint of security it is necessary to require of each system that it remain incapable of solution by an unauthorized person even though the system as such is known, in our present case when the machine and the wheel wirings must be assumed to be known. The Enigma machine Type K by no means satisfies any such security demand, as is obvious from the preceeding parts, since a single correctly guessed word of text can yield the solution of the messa e. The handling of the keys, when correct, can at most make it necessary to solve each message seperately, but can never make the current reading of telegrams impossible. If special auxiliary machines are employed in decipherment it is not even possible to cause any essential delay in the unauthorized decryption. Even a frequent change of the wheel wiring will not satisfy the security requirements. That we are not talking here of excessive security demands will be clear from the supplementary remarks in Part 4 Section C of the present report.

The principle of enciphering the wheels, which is good in and of itself, could only produce results which would satisfy the security

oc ID: 6592459

requirements if the Enigma were entirely reconstructed. Basic requirements for such a reconstruction would be:

1. The regular stepping of the wheels must become quite irregular and appropriate means must be provided for making this stepping subject to setting.
2. The mirror connections must be easily varied by appropriate devices.
3. The entry alphabet must be subject to change by plug connections between the letter keys and the entry wheel.
4. The reciprocal character of the alphabets formed by the machine must be done away with.

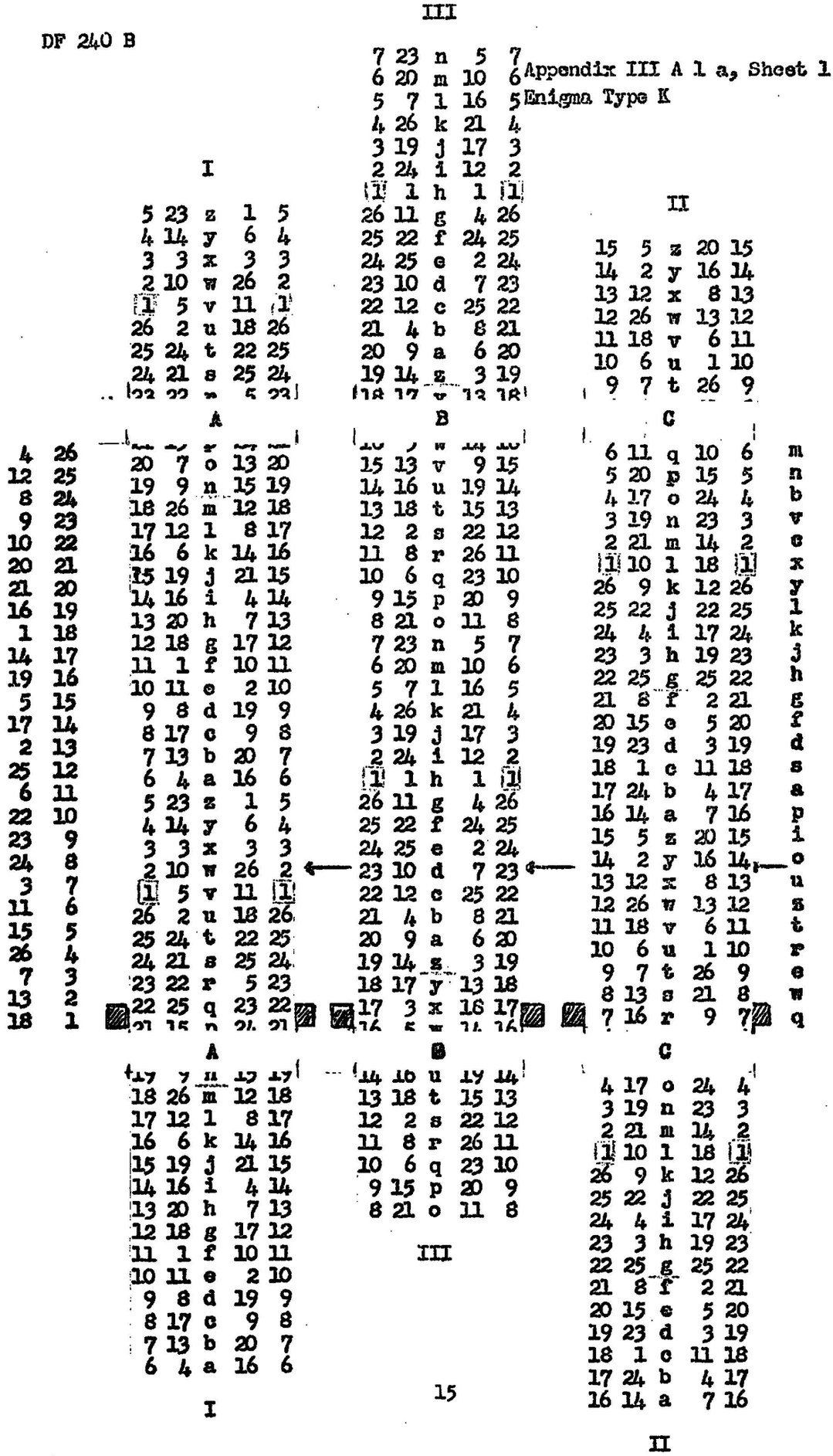
In any case there is no possibility of using the Enigma type K in its present state in a manner which will satisfy security demands.

Of course as a stop-gap measure it would be possible to encipher type K messages again with the same machine or the plain text might first be enciphered by another system and then reenciphered with the Enigma. But such a make-shift solution would not be satisfactory because encipherment and decipherment become too time consuming and simple hand systems might afford greater security and quicker encipherment and decipherment.

Doc ID: 6592459

DF 240 B

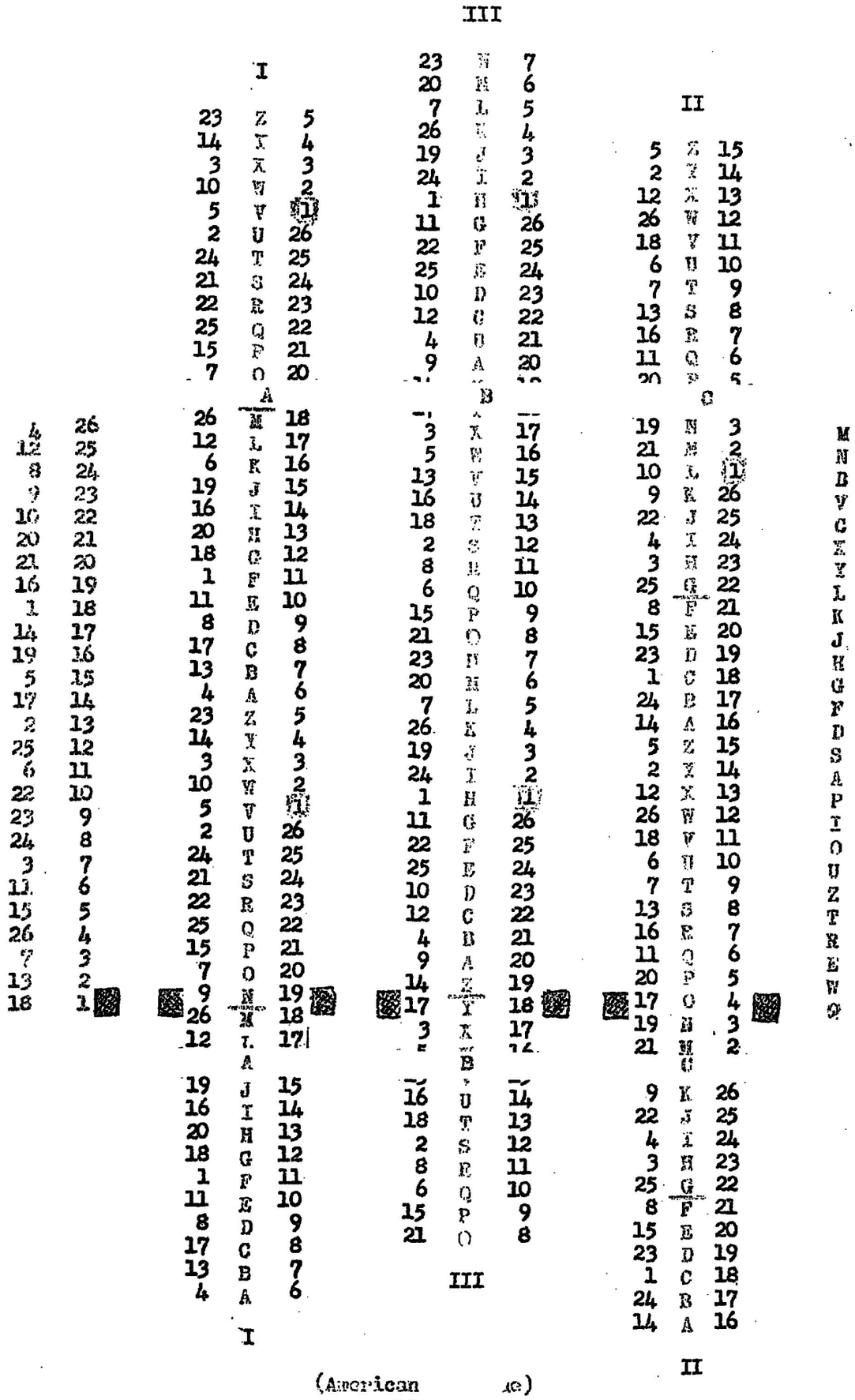
Appendix III A 1 a, Sheet 1
Enigma Type K



15

I, II, III are inverted "sliders" that move up and down.

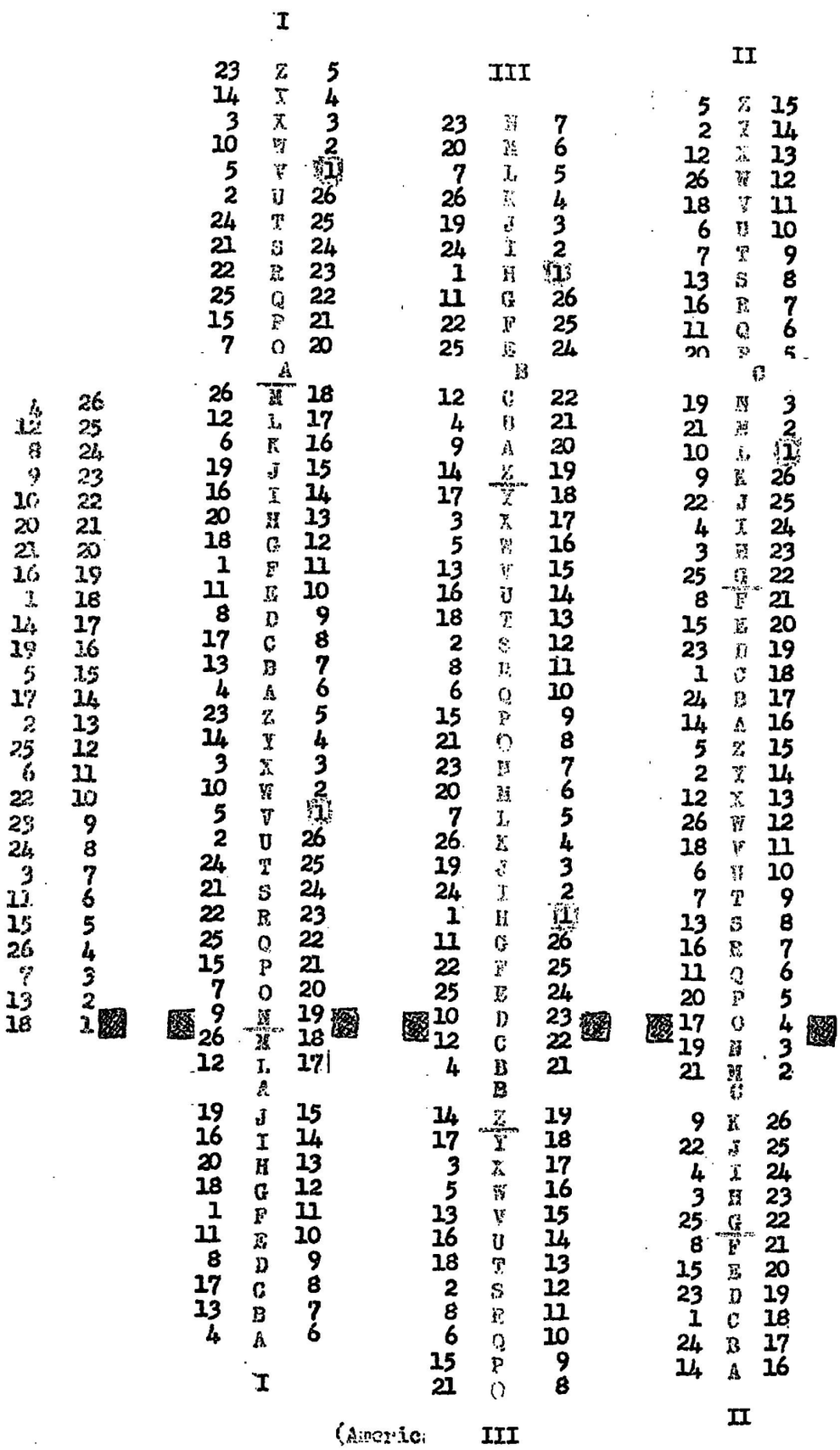
Doc ID: 6592459



16

Columns under I, II, III are "slide rules" that move up & down.

ID: 6592459


I
II
III
M N B V C X Y L K J H G F D S A P I O U Z T R E W Q
(Americ
J
III
II
I
TOP SECRET

Doc ID: 6592459

Appendix III A 1 a, Sheet 2
Enigma Type K

I n																									
III c																									
II f g h i j k l m n o p q r s t u v w x y z a b c d e																									
21 22 23 24 25 26 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20																									
m	e	l	l	i	e	p	w	e	i	v	w	p	z	f	o	b	b	c	h	d	w	e	x	p	q	l	t
n	d	r	t	t	i	c	j	a	v	p	y	z	h	w	d	l	p	b	f	k	r	z	h	c	b	a	g
b	k	j	c	x	e	j	l	i	s	j	p	u	c	e	g	m	m	n	r	c	l	d	r	o	n	r	j
v	f	h	w	o	t	e	e	n	m	b	e	p	t	i	a	f	k	e	s	f	a	u	a	s	f	u	
c	t	t	a	b	m	n	r	j	z	h	l	p	c	r	e	f	h	k	y	g	a	m	j	b	k	m	e
x	b	p	z	b	w	i	s	h	l	p	u	g	c	i	l	x	l	p	p	l	f	f	d	s	f	m	k
y	g	q	r	r	a	t	w	j	z	n	u	g	x	r	o	j	q	u	d	f	q	l	u	z	r	o	x
l	w	m	u	j	b	r	o	x	r	o	j	q	u	d	f	q	l	u	z	r	v	k	q	n	y	h	q
k	r	o	j	k	l	n	c	y	b	a	s	l	u	z	r	u	a	c	i	z	n	g	q	a	q	b	
j	o	b	k	l	n	c	y	b	a	s	l	u	z	r	u	a	c	i	z	n	g	q	a	q	b		
h	a	v	e	g	d	s	o	x	c	s	b	n	d	e	k	i	y	p	b	c	q	u	v	z	x	y	
g	p	e	u	h	b	v	m	w	e	t	i	y	p	b	c	q	u	v	z	x	y	l	v	s			
f	x	e	s	p	e	k	e	s	i	k	o	m	x	t	v	p	n	u	v	z	a	b	l	r			
d	n	t	s	w	h	k	t	r	k	s	t	h	n	u	z	s	t	m	a	b	l	r	s				
s	m	f	d	a	q	h	x	b	f	h	j	w	i	t	w	m	d	o	p	t	i	v					
a	h	c	o	s	y	q	n	u	w	j	q	c	q	r	v	c	j	e	r	d	v	o					
p	e	x	f	q	m	o	z	r	m	x	m	v	o	w	e	n	f	u	h	y	s						
i	u	w	q	n	r	x	b	m	o	f	s	v	s	v	y	h	z	k	j	e	u						
o	j	k	a	v	e	p	h	l	i	u	r	f	f	p	j	k	d	q	e	a							
u	i	z	s	l	z	z	t	a	k	o	y	b	j	m	r	j	q	f	o	d							
z	q	u	x	t	u	u	p	c	y	c	n	m	r	j	q	f	o	d	e								
t	c	d	n	z	v	y	u	d	q	s	w	d	v	s	s	k	x	z									
r	k	n	y	y	f	c	l	p	d	l	d	x	z	z	k	p	b										
e	p	e	h	f	d	o	x	m	y	g	a	m	t	s	n	p											
w	l	i	v	d	x	m	y	g	a	m	t	s	n	p	z												
q	z	y	i	p	s	a	d	k	t	e	a	k	a	l	z	g	r	i	g	t	k	j	m	j	s		

TOP SECRET

Doc ID: 6592459

TOP SECRET

Appendix III A 1 a_5 Sheet 3
Enigma Type K

21	22	23	24	25	26	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
6	13	13	16	4	22	9	3	17	22	4	26	8	2	18	18	16	10	7	22	16	15	4	21	13	25
7	24	25	3	16	11	5	17	4	14	26	10	22	7	13	4	18	8	12	24	15	10	16	18	5	9
15	11	16	15	9	13	3	6	11	17	10	1	16	9	20	20	19	24	16	13	7	24	2	19	24	11
8	10	22	2	25	9	23	19	20	18	23	4	25	3	5	8	12	9	6	8	5	1	5	6	8	1
25	5	18	20	19	24	11	26	10	26	15	5	18	14	9	5	20	11	18	12	20	23	19	15	23	24
18	4	26	18	22	3	6	10	13	4	16	24	23	8	10	12	14	14	2	1	19	20	1	16	10	4
9	21	24	24	5	25	22	11	26	19	1	9	9	16	3	13	15	15	13	4	13	8	8	7	12	10
22	20	20	1	11	18	24	2	15	24	2	11	12	21	19	14	10	21	14	18	14	7	6	8	20	12
24	2	11	11	8	7	8	21	1	7	8	21	13	1	2	15	17	3	19	16	21	26	25	3	14	13
2	18	12	12	13	19	16	14	18	5	6	13	1	26	24	1	5	16	3	26	10	9	21	5	21	18
5	17	23	9	7	6	2	15	16	6	18	19	7	23	15	3	13	20	4	9	11	19	23	26	15	14
14	23	1	10	18	17	20	22	23	25	3	14	14	18	16	21	1	17	21	10	25	11	3	23	4	19
17	6	4	23	12	23	12	23	6	3	12	2	20	15	25	17	4	19	1	17	26	14	14	13	17	26
19	25	6	22	10	12	21	25	24	12	24	25	10	19	1	26	6	25	20	5	18	13	24	14	1	6
20	8	7	5	21	10	15	18	8	10	11	22	3	25	22	22	7	2	17	2	4	25	13	17	26	7
10	16	2	6	14	21	19	1	22	11	21	16	21	24	17	16	11	23	24	7	17	2	17	11	19	21
23	15	8	21	20	2	26	24	19	15	20	17	2	22	23	19	8	1	10	14	6	22	20	1	9	15
1	22	21	19	24	15	18	20	2	8	9	23	6	17	14	10	26	12	11	23	1	21	9	12	25	22
11	12	5	17	23	4	10	13	3	1	13	8	4	20	12	25	25	6	15	6	23	5	18	22	22	23
3	26	9	13	26	26	25	5	12	2	14	18	11	12	7	11	9	4	8	15	3	17	15	4	7	17
21	1	15	25	1	1	4	16	14	16	19	20	24	11	21	7	3	22	22	11	8	12	22	10	6	8
16	7	19	26	17	14	1	7	21	9	22	7	17	6	8	2	2	7	23	21	9	6	12	24	3	20
12	13	14	14	3	16	13	4	7	13	7	15	26	5	11	23	21	18	5	19	22	18	7	25	18	16
4	3	10	8	2	8	17	8	9	21	17	3	15	10	4	24	22	5	25	3	2	16	10	9	16	2
13	3	17	7	15	20	14	9	5	20	25	6	19	4	6	6	23	26	26	20	24	4	26	2	2	3
26	14	3	4	6	5	7	12	25	23	5	12	5	13	26	9	24	13	9	25	12	3	11	20	11	5

TOP SECRET

Appendix III A 1 a, Sheet 4
Enigma Type K

	21	22	23	24	25	26	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
+	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
(20)	6	14	15	19	8	1	15	[10]	25	5	14	11	20	15	6	7	6	1	25	15	10	10	26	18	11	24
19	7	25	1	6	20	16	11	24	[12]	23	10	21	8	20	1	19	8	25	4	17	9	5	12	15	3	8
18	15	12	18	18	13	18	9	13	19	[26]	20	12	2	22	8	9	9	15	8	6	1	19	24	16	22	10
17	8	11	24	5	3	14	3	26	2	1	[7]	15	11	16	19	23	2	26	24	1	25	22	1	3	6	26
16	25	6	20	23	23	3	17	7	18	9	25	[16]	4	1	23	20	10	2	10	5	14	18	15	12	21	23
15	18	5	2	21	26	8	12	17	21	13	26	9	[9]	21	24	1	4	5	20	20	13	15	23	13	8	3
14	9	22	26	1	9	4	2	18	8	2	11	20	21	[3]	17	2	5	6	5	23	7	3	4	4	10	9
13	22	21	22	4	15	23	4	9	23	7	12	22	24	8	[7]	3	26	12	6	11	18	2	2	5	18	11
12	24	3	13	14	12	12	14	2	9	16	17	6	25	14	16	[4]	7	20	11	3	15	21	21	26	12	12
11	2	19	14	15	17	24	22	21	26	14	16	24	13	13	12	16	[21]	7	21	13	4	4	17	2	19	17
10	5	18	25	12	11	11	8	22	24	15	2	4	19	10	3	18	3	[11]	22	2	5	14	19	23	13	13
9	14	24	3	13	22	22	26	3	5	8	13	25	26	5	4	10	17	8	[13]	3	19	6	25	20	2	18
8	17	7	6	26	16	2	18	4	14	12	22	13	6	2	13	6	20	10	19	[10]	20	9	10	10	15	25
7	19	26	8	25	14	17	1	6	6	21	8	10	22	6	15	15	22	16	12	24	[12]	8	20	11	25	5
6	20	9	9	8	25	15	21	25	16	19	21	7	15	12	10	11	23	19	9	21	24	[20]	9	14	24	6
5	10	17	4	9	18	26	25	8	4	20	5	1	7	11	5	5	1	14	16	26	11	[23]	[13]	8	17	20
4	23	16	10	24	24	7	6	5	1	24	4	2	14	9	11	8	24	18	2	7	26	17	16	[24]	7	14
3	1	23	23	22	2	20	24	1	10	17	19	8	18	4	2	25	16	3	3	16	21	16	5	9	[23]	21
2	11	13	7	20	1	9	16	20	11	10	23	19	16	7	26	14	15	23	7	25	17	26	14	19	20	[22]
[1]	3	1	11	16	4	5	5	12	20	11	24	3	23	25	21	26	25	21	26	8	23	12	11	1	5	16
26	21	[2]	17	2	5	6	10	23	22	25	3	5	10	24	9	22	19	13	14	4	2	7	18	7	4	7
25	16	8	[21]	3	21	19	7	14	3	18	6	18	3	19	22	17	18	24	15	14	3	1	8	21	1	19
24	12	20	16	[17]	7	21	19	11	15	22	17	26	12	18	25	12	11	9	23	12	16	13	3	22	16	15
23	4	10	12	11	[6]	13	22	15	17	4	1	14	1	23	18	13	12	22	17	22	22	11	6	6	14	1
22	13	4	19	10	19	[25]	20	16	13	3	9	17	5	17	20	21	13	17	18	13	18	25	22	25	26	2
21	26	15	5	7	10	10	[13]	19	7	6	15	23	17	26	14	24	14	4	1	18	6	24	7	17	9	(4)

TOP SECRET

Doc ID: 6592459

20	6	25	18	5	23	8	2	9	9	14	2	25	6	6	10	5	24	3	7	8	2	1	3	6	26	4
19	7	12	24	23	26	4	4	2	26	15	13	13	22	12	5	8	16	23	26	4	3	13	6	25	9	24
18	15	11	20	21	9	23	14	21	24	8	22	10	15	11	11	25	15	21	14	14	16	11	22	17	11	8
17	8	6	2	1	15	12	22	22	5	12	8	7	7	9	2	14	25	13	15	12	22	25	7	18	3	10
16	25	5	26	4	12	24	8	3	14	21	21	1	14	4	26	26	19	24	23	22	18	24	26	15	22	26
15	18	22	22	14	17	11	26	4	6	19	5	2	18	7	21	22	18	9	17	13	6	10	12	16	6	23
14	9	21	13	15	11	22	18	6	16	20	4	8	16	25	9	17	11	22	18	18	10	5	24	3	21	3
13	22	3	14	12	22	2	1	25	4	24	13	13	23	24	22	12	12	17	1	15	9	13	1	12	8	9
12	24	13	25	13	16	17	21	8	1	17	23	3	10	13	25	13	13	4	25	17	1	22	15	13	10	11
11	2	18	3	26	14	15	25	5	10	10	24	5	3	18	18	21	14	1	4	6	25	18	23	4	18	12
10	5	24	6	25	25	26	6	1	11	11	3	18	12	23	20	24	6	25	8	1	14	15	4	5	12	17
9	14	7	8	8	18	7	24	20	20	25	6	26	1	17	14	7	8	15	24	5	13	3	2	26	13	13
8	17	26	9	9	24	20	16	12	22	18	17	14	5	26	6	19	9	26	10	20	7	2	21	2	13	18
7	19	9	4	24	2	9	5	23	3	22	1	17	17	15	1	9	2	2	20	23	8	21	17	23	2	25
6	20	17	10	22	1	5	10	14	15	4	9	23	20	20	8	23	10	5	5	11	19	4	19	20	15	5
5	10	16	23	20	4	6	7	11	17	3	15	11	8	22	19	20	4	6	6	9	4	14	25	10	25	6
4	23	23	7	16	5	19	19	15	13	6	14	21	2	16	23	1	5	12	11	19	5	6	10	11	24	20
3	1	13	11	2	21	21	23	16	7	5	10	12	11	1	24	2	26	20	21	2	19	9	20	14	17	14
2	11	1	17	3	7	13	20	13	25	23	20	15	4	21	17	3	7	7	22	3	20	8	9	8	7	21
1	3	2	21	17	6	25	13	10	12	26	7	16	9	3	7	4	21	11	13	10	12	20	13	24	23	22
26	21	8	16	11	13	10	15	24	19	1	25	9	21	8	16	16	3	8	19	24	24	23	16	9	20	16
25	16	20	12	10	10	1	11	13	2	9	26	20	24	14	12	18	17	10	12	21	11	17	5	19	5	7
24	12	10	13	7	8	16	9	26	18	13	11	22	25	13	3	10	20	16	9	26	26	16	14	1	4	13
23	4	4	5	19	20	18	3	7	21	2	12	6	13	10	4	6	22	19	16	7	21	26	11	7	1	15
22	13	15	15	6	13	14	17	17	8	7	18	24	19	5	13	15	23	14	2	16	17	12	18	21	16	1
21	26	14	1	18	3	3	12	18	23	16	16	4	26	2	15	11	1	18	3	25	23	7	8	22	14	2

TOP SECRET

TOP SECRET

Doc ID: 6592459

TOP SECRET

17	26
4	25
3	24
19	23
6	22
7	21
12	20
23	19
8	18
26	17
11	16
9	15
5	14
2	13
20	12
16	11
1	10
15	9
18	8
21	7
22	6
14	5
25	4
24	3
13	2
10	1

Reversing mirror of the wheel complex consisting of the reversing wheel
Wheel I
Wheel III
with the window setting n c f

9	18
21	22
21	22
4	14
16	17
14	11
8	26
22	4
10	6
17	13
5	5
6	2
9	18
11	7
18	21
21	22
9	18
20	9
16	17
12	13
10	6
17	
5	
5	
15	
17	

Same reversing mirror, but expressed in the difference values between the contacts.

Row 15
from Sheet 5

10
16
23
20
4
6
7
11
17
3
15
11
8
22
19
20
4
6
6
9
4

Row 5
from Sheet 5

TOP SECRET

Doc ID: 6592459

Doc ID: 6592459

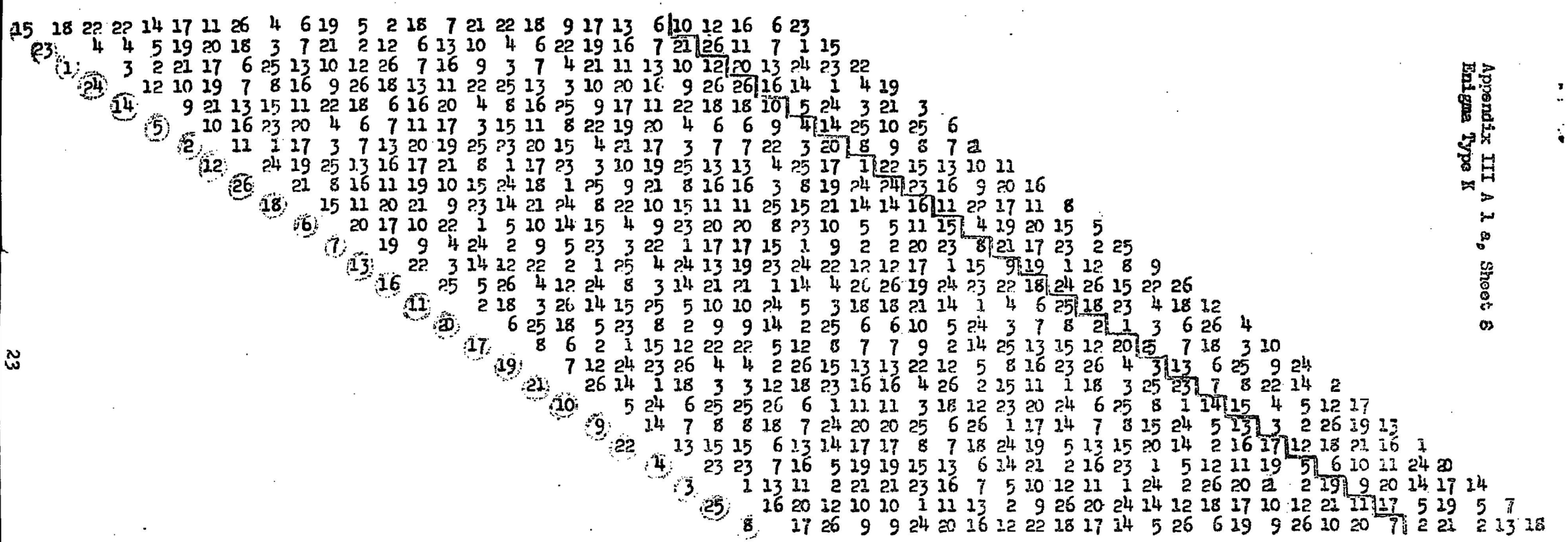
TOP SECRET

15	18	22	22	14	17	11	26	4	6	19	5	2	18	7	21	22	18	9	17	13	6	10	12	16	6	23
23	4	4	5	19	20	18	3	7	21	2	12	6	13	10	4	6	22	19	16	7	21	26	11	7	1	15
1	3	2	21	17	6	25	13	10	12	26	7	16	9	3	7	4	21	11	13	10	12	20	13	24	23	22
24	12	10	19	7	8	16	9	26	18	13	11	22	25	13	3	10	20	16	9	26	26	16	14	1	4	19
14	9	21	13	15	11	22	18	6	16	20	4	8	16	25	9	17	11	22	18	18	10	5	24	3	21	3
5	10	16	23	20	4	6	7	11	17	3	15	11	8	22	19	20	4	6	6	9	4	14	25	10	23	6
2	11	1	17	3	7	13	20	19	25	23	20	15	4	21	17	3	7	7	22	3	20	8	9	8	7	21
12	24	19	25	13	16	17	21	8	1	17	23	3	10	19	25	13	13	4	25	14	1	22	15	13	10	11
26	21	8	16	11	19	10	15	24	19	1	25	9	21	8	16	16	3	8	19	24	24	23	16	9	20	16
18	15	11	20	21	9	23	14	21	24	8	22	10	15	11	11	25	15	21	14	14	16	15	22	17	1	8
6	20	17	10	22	1	5	10	14	15	4	9	23	20	20	8	23	10	5	5	11	15	4	19	20	15	5
7	19	9	4	24	2	9	5	23	3	22	1	17	17	15	1	9	2	2	20	23	8	21	17	23	2	25
13	22	3	14	12	22	2	1	25	4	24	19	19	23	24	22	12	12	17	1	15	9	19	1	12	8	9
16	25	5	26	4	12	24	8	3	14	21	21	1	14	4	26	26	19	24	23	22	18	24	26	15	22	26
11	2	18	3	26	14	15	25	5	10	10	24	5	3	18	18	21	14	1	4	6	25	18	23	4	18	12
20	6	25	18	5	23	8	2	9	9	14	2	25	6	6	10	5	24	3	7	8	2	1	3	6	26	4
17	8	6	2	1	15	12	22	22	5	12	8	7	7	9	2	14	25	13	15	12	22	25	7	18	3	10
19	7	12	24	23	26	4	4	2	26	15	13	13	22	12	5	8	16	23	26	4	3	13	6	25	9	24
21	26	14	1	18	3	3	12	18	23	16	16	4	26	2	15	11	1	18	3	25	23	7	8	22	14	2
10	5	24	6	25	25	26	6	1	11	11	3	18	12	23	20	24	6	25	8	1	14	15	4	5	12	17
9	14	7	8	8	18	7	24	20	20	25	6	26	1	17	14	7	8	15	24	5	13	3	2	26	19	13
22	13	15	15	6	13	14	17	17	8	7	18	24	19	5	13	15	23	14	2	16	17	12	18	21	16	1
4	23	23	7	16	5	19	19	15	13	6	14	21	2	16	23	1	5	12	11	19	5	6	10	11	24	20
3	1	13	11	2	21	21	23	16	7	5	10	12	11	1	24	2	26	20	21	2	19	9	20	10	17	14
25	16	20	12	10	10	1	11	13	2	9	26	20	24	14	12	18	17	10	12	21	11	17	5	19	5	7
8	17	26	9	9	24	20	16	12	22	18	17	14	5	26	6	19	9	26	10	20	7	2	21	2	13	18

TOP SECRET

6592459

Appendix III A 1 a, Sheet 8
Enigma Type K



Doc ID: 6592461

~~TOP SECRET~~

ARMED FORCES SECURITY AGENCY

DF-240 Part I

61/51/~~TOPSEC~~/AFSA-14

Copy No. 35

From: AFSA-14

To: ARCHIVES AFSA 252 H

[THIS DOCUMENT CONTAINS INFORMATION AFFECTING THE NATIONAL DEFENSE OF THE UNITED STATES WITHIN THE MEANING OF THE ESPIONAGE LAWS, TITLE 18, U.S.C., SECTIONS 793 and 794. SEE ALSO PUBLIC LAW 513, 81ST CONGRESS, SECOND SESSION. ITS TRANSMISSION OR THE REVELATION OF ITS CONTENTS IN ANY MANNER TO AN UNAUTHORIZED PERSON IS PROHIBITED BY LAW.]

Approved for Release by NSA on 09-12-2017, FOIA Case #67677

~~TOP SECRET~~

Doc ID: 6592461

DF 240 Part I

61/51/~~TOPSEC~~/AFSA-14

CHARACTERISTICS, ANALYSIS AND SECURITY OF CRYPTOGRAPHIC SYSTEMS

1. Attached is an Armed Forces Security Agency translation of Part I of a treatise on cryptology prepared by Dr. Bruno KRÜGER, formerly with the Forschungsamt. German title: Systematik, Analyse und Sicherheit der Geheimschriften.

2. This treatise purports to cover in detail the work given in the course of the Forschungsamt. Since the methods described in this part are not essentially different from those used by AFSA, the primary value will be found in the picture it gives of the approach to these problems of another major cryptologic unit. In some cases fresh points of view may be noted. The "Appendices" have been inserted at the end of each section.

3. Other parts will follow.

Translated: R.W.P.
August 1951
Distribution: Normal

35 copies

175 pages

Doc ID: 6592461

TABLE OF CONTENTS

	Page
Introductory Remarks	6
I. Basic systems	7
Grundverfahren	
A. Substitution systems	7
Ersatzverfahren	
1. Simple letter substitution	7
Einfacher Buchstabencäsar	
a) Standard alphabet	
Systematischer Cäsar	
b) Reciprocal (reversed) alphabet	
Reziproker Cäsar	
c) Random alphabet	
Unsystematischer Cäsar	
2. Simple digit substitution	22
Einfacher Zahlencäsar	
3. Digit substitution with variants	26
Mehrfach belegter Zahlencäsar	
a) Substitution with few variants	
Schwach mehrfach belegter Cäsar	
b) Syllabic substitution	
Silbencäsar	
4. Digraphic substitution	36
Der Paarcäsar	
a) German digraphic substitution	
Deutscher Paarcäsar	
b) English digraphic substitution	
Englischer Paarcäsar	
c) Reconstruction of the square of the English digraphic substitution	
Rekonstruktion des Schlüsselquadrats des englischen Paarcäsars	

Doc ID: 6592461

		Page
5.	Substitution with nulls	52
	Cäsar mit Blender	
	a) Random nulls	
	Unsystematischer Blender	
	b) Systematic nulls	
	Systematischer Blender	
6.	Monome-dinome substitution	59
	Wechselstelliger Zahlencäsar	
7.	Polyalphabetic substitution with interrupted period	65
	Der Springcäsar	
	a) Systematic interval	
	Systematischer Sprungabstand	
	b) Random interval	
	Unsystematischer Sprungabstand	
8.	Periodic polyalphabetic substitution	77
	Der Spaltencäsar	
	a) With short slide	
	Mehrspaltencäsar mit kurzem Schieber	
	b) With long slide	
	Mehrspaltencäsar mit langem Schieber	
	c) Tritheim table and derived tables	
	Tritheim'sche Tabelle und davon abgeleitete Tabellen	
	d) Communist system	
	Kommunistenverfahren	
	e) Encipherment with a key book	
	Buchverschlüsselung	

Doc ID: 6592461

Pages

9. Reduction of polyalphabetic substitutions 104

Reduktion von Spalten- und Springcäsaren

a) Short slide

Kurzer Schieber

b) Long slide

Langer Schieber

c) Route

Duktus

d) Constructive parallel passages

Konstruktive Parallelstellen

10. Periodic polyalphabetic substitution with selective encipherment. 133

Spaltencäsar mit Wahlverzifferung

11. Code 136

Der Code

a) Size and group structure

Umfang und Gruppenaufbau

b) Meanings

Codebelegung

c) Count and solution

Statistik und Lösung

B. Transposition Systems 150

Versatzverfahren

1. The limited (short) key number 150

Die begrenzte Umstellzahl

2. Transposition matrix 158

Der Würfel

3. The grille 165

Der Raster

Introductory Remarks.

For the purpose of this study a communication will be regarded as composed in a cryptographic system when

1. Its character as a communication is plainly to be recognized,
2. The communication consists of ordinary letters or new characters which have been agreed upon in advance, but
3. The sequence of these characters is not intended to yield meaningful words or sentences for a third party.

The purpose of the cryptogram is then that it shall be readable for the sender and receiver but not for third parties - particularly during transmission.

Excluded from the study are all methods of secret transmission of communications where the communication is not recognizable as such by third parties, for instance where invisible inks are used, or where there is no written fixation, for instance in case of speech scrambling. For the essence of the cryptographic system it makes no difference which language and which characters are employed or in which way the communications are sent. The question of how an encrypted communication is sent plays a role only when the security of cryptograms against unauthorized reading is being studied.

Doc ID: 6592461

PART I

BASIC SYSTEMS

When the secret text which is to be transmitted can be developed from the underlying plain text in a single procedure, then such systems are called basic systems (Grundverfahren).

If, on the other hand, the secret text has been developed from the plain text by two more more procedures, one after the other, we then speak of combined or superenciphered systems (Kombinierte oder überschlüsselte Verfahren).

From the standpoint of the study of characteristics it makes no difference whether the cryptogram is developed from the plain text manually or by the aid of a particular cipher machine, i.e. whether a hand system or a machine system is involved. If in the course of this study cipher machines are treated in a special section, this is not due to characteristics but simply to practical considerations, in particular to their analysis and the multiplicity of technical possibilities which exist.

Section A.

Substitution Systems

(Ersatzverfahren)

According to the method employed to convert the plain text into a cipher text, cryptographic systems are divided into substitution and transposition systems.

A substitution system is involved when the individual elements of the plain text are replaced by other elements of the cipher text but remain in their natural sequence. On the other hand with a transposition system the individual elements of the plain language are preserved but are taken out of their natural sequence and transposed with respect to one another according to definite rules.

1. Simple substitution. (Einfacher Cäsar)

The simplest of all substitution systems and possibly the oldest of all

cryptographic procedures, where each element of the plain language - be it letter, number, punctuation mark or a combination of these - is replaced in its natural sequence by a cipher element, is called a Cäsar (simple substitution). This name is due to the fact that it was assumed - whether rightly or wrongly we need not determine - that in ancient times Caesar was the first person to make use of this cryptographic system.

According to whether letters or digits are used as cipher elements we speak of letter substitution or digit substitution. The use of any other symbols in place of letters or digits may be disregarded because they do not cause any difference in character and such attempts are without any practical significance and are only proposed by laymen.

The letter system is to be preferred to the digit system when it is a question of keeping the cipher text as short as possible, for instance to keep down telegraph charges, because compared with the use of digits the use of letters affords

2-1/2 times as many possibilities when taken one at a time
6-1/2 " " " " " " two " " "
17-1/2 " " " " " " three " " "
more than 45 " " " " " " four " " "

On the other hand, digits have an advantage over letters in that they are easier, quicker and surer to handle, particularly in the case of all superencipherments. For this reason letters predominate in machine systems, because here the work is done by the machine, whereas in the case of hand systems preference may frequently be given to digits.

In the following examples of the structure of substitution alphabets:

Plain sequence:	a b c d e f g h i j k l m n o p q r s t u v w x y z
Cipher sequence 1:	x y z a b c d e f g h i j k l m n o p q r s t u v w
Cipher sequence 2:	z y x w v u t s r q p o n m l k j i h g f e d c b a
Cipher sequence 3:	g o y j v n a p z d l k s f b h w x m u t e q r c i
Cipher sequence 4:	e j o t y d i n s x c h m r w b g l q v a f k p u z
Cipher sequence 5:	m q f o p c k r l j z a s g t n b u d v w e h y i x

cipher sequence 1 represents a standard alphabet (with a displacement of 3) (alphabetischen Cäsar im Verschiebungsgrad 3); cipher sequence 2 a reversed and reciprocal alphabet (alphabetisch rücklaufigen und reziproken Cäsar), cipher sequence 3 a reciprocal alphabet (reziproken Cäsar), cipher sequence 4 a systematically mixed alphabet (alphabet at an interval of 5) (systematischen Cäsar (Alphabet im Abstand 5 enthalten)), and cipher sequence 5 represents a random alphabet (unsystematischen Cäsar). Digit substitutions may be developed in corresponding fashion whereby the alphabetic arrangement is replaced by an arithmetic arrangement. In addition, with systematic digit substitutions it is possible to derive the sequences from the digit square using a key word (Schlüsselwort) or a route (Duktus) as is shown in the Appendices.

At this point it may be remarked that it will be well, while reading the following pages, to take out an appendix as mentioned and to keep it spread besides the text until the following appendix is mentioned.* Constant comparison of the text and the explanatory example should greatly facilitate comprehension.

In Appendix I A 1 a we have on sheet 1 a plain text converted into cipher text with the aid of the substitution alphabet (normal) shown at the top of sheet 2. In order to determine the security of such a system against unauthorized decipherment, i.e. against decipherment by third parties, it is necessary to subject the cipher text to a somewhat detailed study. For this purpose the cipher text of this simple letter substitution has been subjected to a so-called biliteral count (einstellige Kettenstatistik, literally, 1-place chain count) in the following manner:

At the left margin of sheet 2 of the appendix the possible cipher elements from a to z have been entered in alphabetic sequence one beneath the other on 26 lines and in each case represent the first member of a link of this chain count which is undertaken as follows. Of the cipher text beginning hgekxtc... etc., the first two elements hg are taken first, then the elements in second and third position ge, then the elements in third and fourth position ek etc.

---

* Note: These have been bound in at the end of each section.

and counted so that in row h (first link) a 'g' (second member of a link) is entered, in row g an 'e', in row e a 'k' etc. with the appropiate row index from 1 to 7. The entry g_1 in row h signifies therefore that the sequence of cipher letters hg appears in the first row of the cipher text. The entry x_1x_1 in row k signifies that the cipher digraph kx appears twice in the first line of the cipher text. In the same manner as this repeated digraph longer repeats in the cipher text are revealed by the count. These repetitions in the cipher texts are called parallel passages and are regularly marked in the same manner, using colored pencil. Moreover an index number beneath this marking shows in which lines of the cipher text the other parallel passages are to be sought.

In this connection it is generally well to consider as parallel passages and to mark as such in the cipher text only repetitions with a definite minimum length. In this way we make sure that only those repetitions in the cipher text are considered as parallel passages to which a repetition in the plain text corresponds. This minimum length will have to be determined variously, depending on the cryptographic system and on the amount of material to be studied. In the present system, the simple letter substitution, even the shortest parallel passages, namely digraphs, may be taken into account because in this system only genuine parallel passages occur where a repetition in the plain text does correspond to the repetition in the cipher text. The chain count carried out in the manner described has been evaluated on sheet 2 of the appendix by adding up the number of entries in each row, i.e. for each cipher letter, separately. This number shows how frequently the particular letter has appeared in the cipher texts, while the entries on the line itself indicate the other cipher elements in connection with which the one under study occurs. Thus it may be important for interpretation to know which cipher elements occur repeatedly paired with themselves, because in a text in the German language these might suggest the digraphs ss, ll, mm, etc, or which cipher elements enter into combinations with definite other elements primarily, whether these second elements are rare or frequent, and many other things.

In the tabulation at the bottom of sheet 2 the cipher elements are arranged according to their frequency in the cipher text, in which connection the number of different cipher elements is also shown. Finally on sheet 3 the parallel passages are listed with an indication of their position in the text by row and column, their length and their intervals from one another. Intervals and lengths of parallel passages are always calculated according to individual elements. Intervals are counted from the beginning of the first parallel passage to the beginning of the second parallel passage.

From this we get for the present simple substitution the following analysis:

1. The number of different cipher elements found in a text of 200 elements is 20.
2. The cipher elements show plain-text frequency.
3. The parallel passages occur with plain-text frequency.
4. The length of the parallel passages is not regular.
5. The interval between parallel passages is not regular.

This result corresponds with that which would result from a study of the appropriate plain text. Nothing else was to be expected because by a simple substitution a particular plain element is always replaced by another particular cipher element, so that the over-all picture, taken as such, has not changed, aside from the fact that the sequences of letters no longer make sense.

The solution of such a cipher text by an unauthorized person, i.e. without knowledge of the substitution on which the encipherment is based, is correspondingly simple. It requires nothing more then a little talent for putting two and two together, plus a knowledge of the frequencies of the several plain elements and of the frequent digraphs and trigraphs of the language, a knowledge which can be obtained by a count of a suitable plain text of adequate length. This table of frequencies, which turns out slightly different for each language corresponding to its peculiarities, is assumed to be known, as is the arrangement of the plain letters according to their frequency, which in German runs e n i r s t u d a h .....etc.

If we begin by replacing by an e the most frequent cipher letter k in our text, which on the basis of its outstanding frequency can immediately be interpreted as e, we have left as equivalent for plain n the cipher elements txozj and possibly y on the basis of their frequency. If we first try the assumption that cipher t is equal to plain n, because

1. t is the second most frequent cipher element, and
2. Both the cipher digraph kt and the cipher digraph tk (plain en and ne) are frequent, then we get in line 2, columns 11 to 17, of the appendix the following picture:

Interpretation: . n . e n e n

Cipher text: o t j k t k t ,

which automatically leads us to fill in "in denen".

This interpretation gains in plausibility through the fact that this passage would correspond to the parallel passage "otjkt", which would read "in den" and the parallel passage "jkt" which would correspond to the article "den", of which the former occurs once more and the latter occurs four more times in the cipher text. Therefore, if on the basis of this passage we interpret cipher o = plain i and cipher j = plain d, which is not unlikely in view of the frequencies 17 and 14 respectively, then upon entering these interpretations we find no contradictions, for instance the text in line 4 column 13 following, shows:

Interpretation: e den die e i en nde ndd ei

Cipher text: ckxjktyzuvjokxkhxomktnatjkxzatjjxko

e dne en e deninden .....

ghmkuxjtkzktckxjktotjkt .....

Having obtained for the most frequent letters the following interpretations:

plain e n . i d d .

cipher k t x o z j y , the cipher elements x z y remain as plausible for the next most frequent letters r s t.

This possibility, taken with the text above, yields for the parallel passage

e den the interpretation werden . Then the passage nder nddrei leads
ckxjkt ckxjkt natjkxzatjjxko

us to guess "hundertunddrei", so that cipher a = plain u, cipher z = plain t and cipher n = plain h. The rest of the interpretation follows of necessity.

Moreover the interpretations thus far made:

Cipher sequence: abcdefghijklmnopqrstuvwxyz

Plain sequence: u w de i n r t

when scrutinized closely reveal that the plain sequence is alphabetic so that the remaining interpretations can be supplied without further ado.

The example given in the next appendix I A 1 b shows a substitution characterized by an alphabet which runs backward in the cipher sequence and by the fact that the individual values are reciprocal, i.e. if plain e = cipher v, then conversely plain v = cipher e. The analysis shows the same characteristics as the example in the preceding appendix; however the tabulation of the cipher elements according to their frequency on sheet 2 at the bottom shows that with relatively short texts - although the present text has 119 elements - marked deviations from the average frequency may occur. Thus in this example the relative order of frequency of e and n is the reverse of the normal; letters like l d a are here more frequent than i r s t . Nevertheless the interpretation of the cipher text is not rendered much more difficult, if the parallel passages and digraphic frequencies are given due consideration; The cipher digraph xs, which occurs five times, suggests, if we consider the fact that x does not begin any other digraphic combination, the interpretation ch, assuming that the underlying language is German. Interpretation is greatly facilitated as soon as the reciprocal character of the substitution is recognized.

The text enciphered in Appendix I a 1 c with a random alphabet merely confirms what has been recognized thus far and shows that even a completely random substitution alphabet is very easy to solve.

Doc ID: 6592461

~~TOP SECRET~~

IA 1a

0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0

Klartext / Plain text: b a y e r n w i r d i n h ü n d e r t s t e i n k r e i s e

Geheimtext / Cipher text: h g e k x t c o x j o t n a t j k x z y z o s s q x k o y k 1

Klartext / Plain text: e i n g e t e i l t i n d e n e n h ü n d e r t a b g e o r

Geheimtext / Cipher text: k o t m k z k o r z o t j k t k t n a t j k x z g h m k ü x 2

Klartext / Plain text: d n e t e a l s v e r t r e t e r i h r e s s t i m m k r e

Geheimtext / Cipher text: j t k z k g r y b k x z x k z k x o n x k y y z o s s q x k 3

Klartext / Plain text: i s e s g e w a e h l t w e r d e n s t o p d i e ü e b r i

Geheimtext / Cipher Text: o y k y m k c g k n r z c k x j k t y z ü v j o k a k h x o 4

Klartext / Plain text: g e n h ü n d e r t ü n d d r e i a b g e o r d n e t e n v

Geheimtext / Cipher Text: m k t n a t j k x z a t s j j x k o g h m k ü x j t k z k t c 5

Klartext / Plain text: e r d e n i n d e n w a h l k r e i s e n a ü s d e n w a h

Geheimtext / Cipher Text: k z j k t o t j k t c g n r q x k o y k t g a y j k t c g n 6

Klartext / Plain text: l k r e i s l i s t e n g e w a e h l t

Geheimtext / Cipher Text: r q x k o y r o y z k t m k c g k n r z 7

= 200 Elemente

IA 1a - 1

— 1 —

~~TOP SECRET~~

Doc ID: 6592461

Einfacher Buchstabencäsar, alphabetisch (1 Bl.)
Simple Monoalphabetic Substitution - Standard Alphabet

Klardoppelte Plain elements	a b c d e f g h i j k l m n o p q r s t u v w x y z
Geheimelemente Cipher elements	g h i j k l m n o p q r s t u v w x y z a b c d e f

Einstellige Kettenstatistik des Geheimtextes
Digraphic count of cipher text, with frequencies

	1 2 3 4 5 6 7 8 9 10	1 2 3 4 5 6 7 8 9 20	1 2 3 4 5 6 7 8 9 30	Häufigkeit Frequency der Belegung
a	t_1 t_2 k_4 t_5 t_6 y_6			6
b	k_3			1
c	o_1 z_4 k_4 k_5 z_6 z_6 z_7			7
d				-
e	k_1			1
f				-
g	e_1 k_2 r_3 k_4 t_5 n_6 a_6 n_7 k_7			9
h	z_1 n_2 z_4 n_7			4
i				-
j	o_1 k_1 k_2 k_3 t_3 k_4 o_5 k_5 j_5 z_5 t_5 k_6 b_6 k_6			14
k	x_1 z_1 o_1 k_1 o_2 z_2 o_2 k_2 k_2 x_2 n_2 z_2 y_3 z_3 z_3 x_3 y_3 o_3 y_4 c_4 n_4 x_4 t_4 a_4 k_4 t_5 x_5 o_5 n_5 z_5			41
l	t_5 z_5 k_5 t_5 n_5 t_6 k_6 o_6 k_6 z_7 n_7			-
m	k_2 k_2 k_3 k_5 k_5 k_6			6
n	a_1 a_2 z_3 r_4 a_5 r_5 r_6 r_6			8
o	x_1 t_1 k_1 y_2 t_2 r_2 t_2 n_3 s_3 y_4 k_4 n_4 z_5 t_6 y_6 y_6 z_6			17
p				-
q	x_1 x_2 x_4 x_6			4
r	z_1 y_3 z_4 q_4 q_7 o_7 z_7			7
s	s_1 z_2 b_3 z_7			4
t	c_1 n_1 y_2 n_3 y_3 k_3 n_3 j_3 k_3 y_4 n_5 j_5 c_5 k_5 j_5 o_5 j_5 c_5 j_5 c_5 n_5			21
u	z_2 v_4 z_7			3
v	y_4			1
w				-
x	t_1 j_1 z_1 k_2 z_2 j_2 z_3 k_3 o_3 k_3 k_3 j_4 o_4 z_5 k_5 j_5 q_5 k_5 k_5			19
y	z_1 k_1 t_3 y_3 z_3 k_4 n_4 z_4 k_4 k_6 r_7 z_7			12
z	y_1 o_1 k_2 o_2 y_2 k_3 z_3 k_3 o_3 n_4 μ_4 a_5 k_5 k_7			15

Geheimelemente nach Häufigkeit geordnet:
Cipher elements in order of frequency:

Geheimelemente cipher element	k t x o z j y g n c r a m h q s ü b e v	= 20 elements Elemente
Häufigkeit frequency	41 21 19 17 15 14 12 9 8 7 7 6 6 4 4 4 3 1 1 1	
Klarbuchstabe plain equivalent	e n r i t d s a h [illegible] l ü g b k m o w y p	

IA1a-2

Doc ID: 6592461

Parallelstellen

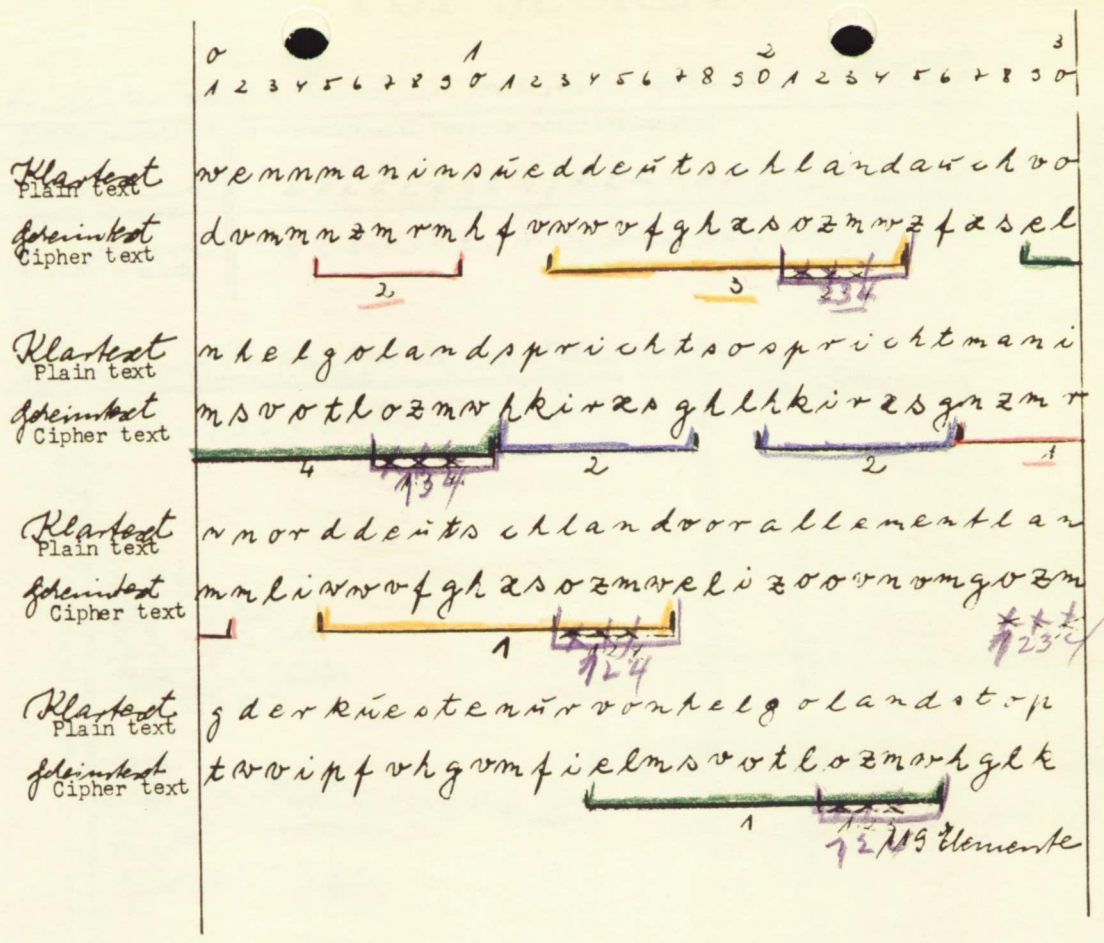
Parallel passages = repeats

Geheimtext cipher	Stellung position	Länge length	Abstände intervals
tnatjkszz	1/2. 2/17. 5/3	8 = 2.2.2	35. 111. 76. = 5.7 = 3.37
ktnatjkszz	2/17. 5/3.	9 = 3.3	76. = 2.2.19
yzoss	1/20. 3/23	5 = 5	63. = 3.3.7 = 2.2.5.7
qzkoyk	1/25. 3/28. 6/15.	6 = 2.3	63. 140. 77. = 7.11
otjkt	2/11. 6/6.	5 = 5	115. = 5.23
gfmtuxjtksk	2/5. 5/18.	11 = 11	83. = 83
mkcgknrz	4/5. 7/13	8 = 2.2.2	98. = 2.7.7
ckzjkt	4/13. 5/30.	6 = 2.3	47. = 47
jktcgnr	6/8. 6/25.	7 = 7	17. = 17

I A 1 a - 3

Doc ID: 6592461

~~TOP SECRET~~



Parallelstellen
Parallel passages = repeats

Geheimtext Cipher text	Stellung Position	Länge Length	Abstände Interval
nvmvm	1/5 . 2/27	5 = 5	52 = 2·2·13
vvvfghzsozmvv	1/13. 3/5.	12 = 2·2·3	52 = 2·2·13
kirzsg	2/11 . 2/20	7 = 7	9 = 3·3
elmsvotlozmvv	1/29 . 4/14	12 = 2·2·3	75 = 3·5·5
ozmvv	1/21 . 2/7	4 = 2·2	16 = 2·2·2·2
"	1/21 . 4/22		91 = 7·13
ozm	3/13 . 3/28	3 = 3	15 = 3·5

I A 1 b - 1

~~TOP SECRET~~

IA1b
IA1c

Doc ID: 6592461

~~TOP SECRET~~

Einfacher Buchstabencäsar, reziprok, systematisch (10 Br)

Simple substitution - reciprocal reverse normal alphabet

Klartelemente ~~Plain element~~	a b c d e f g h i j k l m n o p q r s t u v w x y z.
Geheimelemente Cipher element	z y x w v u t s r q p o n m l k j i h g f e d c b a

Einstellige Kettenstatistik des Geheimtextes.

Digraphic Count

Frequency Häufigkeit

	1	2	Frequency
a			-
b			-
c			-
d	v_1		1
e	$l_1\ l_3\ l_4$		3
f	$v_2\ g_4\ z_1\ z_3\ x_4\ i_4$		6
g	$h_1\ h_2\ n_2\ h_3\ o_3\ v_4\ l_4$		7
h	$f_1\ z_1\ k_2\ k_2\ k_3\ z_1\ g_4\ g_4$		8
i	$r_2\ r_2\ v_3\ z_3\ k_4\ o_4$		6
j			-
k	$i_2\ i_2$		3
l	$m_2\ o_2\ h_2\ i_3\ i_3\ m_4\ o_4\ b_4$		8
m	$m_1\ m_1\ r_2\ h_1\ x_2\ s_2\ v_2\ r_3\ m_3\ l_3\ v_3\ g_3\ t_3\ f_4\ s_4\ x_4$		16
n	$z_2\ z_2\ v_3$		3
o	$z_1\ t_2\ z_2\ z_3\ o_3\ v_3\ z_3\ t_4\ z_4$		9
p	f_4		1
q			-
r	$m_2\ x_2\ x_2\ m_3$		4
s	$o_2\ e_2\ v_3\ g_3\ g_3\ o_3\ v_4$		7
t	$t_2\ v_4\ h_4$		3
u			-
v	$m_1\ v_2\ f_2\ o_2\ t_3\ n_3\ m_3\ i_4\ h_4\ m_4\ o_4$		11
w	$v_1\ v_2\ z_2\ h_2\ v_3\ v_3\ g_3\ v_4\ h_4$		9
x	$o_1\ o_2\ o_2\ h_2\ o_3$		5
y			-
z	$m_1\ m_2\ f_2\ m_2\ m_2\ m_3\ o_3\ m_3\ m_4$		9

Cipher elements in order of frequency

Geheimelemente nach Häufigkeit geordnet

Geheimelemente Cipher elements	m v o r z h l g s f i x e n t k d p	= 19 Elemente elements
Häufigkeit Frequency	16 11 9 9 9 8 8 7 7 6 6 5 4 3 3 3 2 1 1	
Klartedeutung Plain equivalent	n e l d a s o t h ü r c i v m g p w k	

I A 1 b -2

~~TOP SECRET~~

Doc ID: 6592461

~~TOP SECRET~~

0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0

Klartext / Plain text: die sorgfältige anordnung der einzelnen

Geheimtext / Cipher text: vgmvqnpmifmgomlivnmgetmovmtqrs 1

Klartext / Plain text: vers orgfältig darf nicht dazu führen

Geheimtext / Cipher text: jmnvqnpiopvlnbogetzvlsibimtnmo 2

Klartext / Plain text: holzaufschichtenstandardverfahren

Geheimtext / Cipher text: tqrslivsivetlrzmoiovlovmnmzmnc 3

Klartext / Plain text: stoffeinzelfuhrenstopholzistan

Geheimtext / Cipher text: vzqtbmmgosibimtnmovzqatqrsgvzl 4

Klartext / Plain text: derenverkaufsstoffenüberlegenxyz

Geheimtext / Cipher text: ovmnmozmnczvzqbbmoimümnrmpmodhs 5

= 150 Elemente / elements

IAlc-1

~~TOP SECRET~~

IAlc

Doc ID: 6592461

~~TOP SECRET~~

Simple substitution - random alphabet.
Einfache Buchstabencäsar, unsystematisch

Plain elements / Klarelemente	a b c d e f g h i j k l m n o p q r s t u ü v w x y z
Cipher elements / Geheimelemente	l ü e w m b p t g k c r f o q a y n v x i j z d h s

Digraphic count / Buchstabenstatistik des Geheimtextes

	0 1 2 3 4 5 6 7 8 9	10 11 12 13 14 15 16 17 18 19	20 21 22 23 24 25 26	Frequency / Belegung
a	t_4			1 ✓
b	$o_2 i_2 b_4 m_4 i_4 b_5 m_5$			7 ✓
c	$w_3 v_5$			2 ✓
d	h_5			4 ✓
e	$k_1 t_2 t_3$			3 ✓
f	m_1			1 ✓
g	$m_1 o_1 k_1 k_2 o_4 v_4$			6 ✓
h	b_5			1 ✓
i	$f_1 v_1 o_2 b_2 m_2 v_2 v_3 o_3 b_4 m_4 m_5$			11 ✓
j	m_2			1 ✓
k				— ✓
l	$i_1 m_2 s_2 i_2 r_3 o_3 o_4$			7 ✓
m	$v_1 i_1 g_1 l_1 g_1 o_1 t_1 m_2 t_2 o_2 o_3 n_3 z_3 n_3 m_4 g_4 t_4 o_4 n_5 o_5 n_5 b_5 i_5 r_5 f_5 o_5$			26 ✓
n	$f_1 m_1 w_2 f_2 b_2 m_2 m_3 c_3 m_4 m_5 c_5 r_5$			12 ✓
o	$m_1 w_1 f_2 g_2 t_2 i_3 v_3 v_3 b_4 v_4 v_5 z_5 i_5 d_5$			14 ✓
p	$m_1 i_2 v_2 m_3$			4 ✓
q	$m_1 r_1 m_2 r_2 b_4 a_4 r_4 b_5$			8 ✓
r	$s_2 s_2 z_3 s_4 m_5$			5 ✓
s	$g_1 i_2 l_2 i_3 i_4 g_4 - 5$			7 ✓
t	$m_1 g_1 z_2 m_2 g_3 l_3 n_4 g_4$			8 ✓
ü	m_5			1 ✓
v	$g_1 m_1 g_2 s_2 e_3 z_4 z_4 z_4 z_5$			9 ✓
w	$g_1 m_2 l_2 l_2 l_3 m_3 m_5$			7 ✓
x	$v_2 m_3 g_4 g_4 l_4 g_5$			6 ✓
y				e ✓
z	$m_3 m_5$			2 ✓

Geheimelemente nach Häufigkeit geordnet
Cipher elements in order of frequency

Geheimelemente / Cipher elements	m o n i v g t b l s w ü r p e c z a d f h j ü	= 24 Elemente / elements
Häufigkeit / Frequency	26 14 12 11 9 8 8 7 7 7 7 6 6 5 4 3 2 2 1 1 1 1 1 1	
Klarbedeutung / Plain equivalents	e n r ü s o h f a z d i t l g c k v p x m y v b	

I A 1 c - 2

~~TOP SECRET~~

Doc ID: 6592461

Parallel passages = repeats
Parallelstellen

Geheimtext Cipher text	Stellung Position	Länge Length	Abstände Interval
vgnp	1/4. 2/4.	4 = 2.2	30 = 2.3.5
mgo	1/11. 4/7	3 = 3	86 = 2.43
liv	1/15. 3/5.	3 = 3	50 = 2.5.5
get	1/20. 2/16	3 = 3	26 = 2.13
ovm	1/24 3/22	3 = 3	88 = 2.2.2.11
tqrs	1/22 3/01.	4 = 2.2	34 = 2.17
	4/23.	-	86 = 2.43 52 = 2.2.13
sibimtmmo	2/22 4/10.	9 = 3.3	48 = 2.2.2.2.3
mov	3/16, 5/16	3 = 3	60 = 2.2.3.5
[illegible]	3/21. 4/30	6 = 2.3	39 = 3.13
[illegible]	3/22. 5/4	10 = 2.5	40 = 2.2.2.5
vzq	4/07. 4/19	3 = 3	18 = 2.3.3
	5/11	-	40 = 2.2.2.5 22 = 2.11.

IA1c-3

Doc ID: 6592461

2. Simple digit substitution (Einfacher Zahlencäsar)

In Appendix I A 2 a simple random digit substitution is introduced as example. This substitution, in contrast to the one-place letter substitution, is two-place, because only thus do we have enough cipher elements to cover the 26 plain elements. On the other hand we thus get the possibility of including punctuation marks like period and comma or frequent digraphs like ch which when enciphered with two cipher elements greatly facilitate breaking into the substitution.

Before undertaking the usual chain count, whose individual members are here two-place, it is well to determine by a special count made in a digit table, which two-place cipher elements have been used for encipherment. In contrast to letter systems it is not always certain a priori with digit substitutions what the structure of the substitution alphabet may be. Such a count has been made on sheet 1 of the Appendix by entering in the digit table with the coordinates from 0 to 9 a stroke for cipher 92 in that cell of the square which is formed by the 9th column and 3rd row.

In all cases in which the cipher elements consist of several digits or letters, in the present case of two digits, we may also speak of cipher groups or for short of groups or of letter or digit groups. By group we then understand that combination of two or more letters or digits which has a plain meaning of its own.

Consequently the count just mentioned may also be termed a group count. It is characteristic of the group count that each cipher group has a corresponding line or a corresponding cell of its own. On this line is entered, in contrast to the chain count, merely the place in the cipher text where this group has occurred. If in this group count we are only concerned with determining which cipher groups occur or what the frequency of the individual groups is, then the position index may be replaced by a cross or a stroke for each occurrence. In the latter case the group count may be called a frequency count.

In computing the lengths and the intervals of parallel passages we must

remember in the present example that the individual elements 0 to 9 and not the dinomes 00 to 99 are to be counted. As a result, when we break up the values for length and interval into the least factors the number 2 will be a common factor. The dinome substitution therefore has a regular feature to the length of and the interval between parallel passages. The solution of the cipher text itself is carried out in the same way as in the preceding examples.

In respect to security the examples given in appendices I A 1 a , b, c and I A 2 are approximately equal although obviously the security of a substitution with a normal alphabet or a reciprocal alphabet is less than that of one with a random alphabet. It is a common property of all the simple substitutions that the plain text structure is completely preserved in the cipher text; the result of this is that a cipher text enciphered by such a substitution with a total length of 25 letters or less, that is less than one line of text, can still be deciphered so that the correctness of the interpretations may be proved. Moreover much shorter texts can be solved, although in that case it is not possible to prove the validity of the solution and there may be two or more possible interpretations. This means that the simple substitution does not usually have the degree of security demanded for transmitting even a short message.

Doc ID: 6592461

~~TOP SECRET~~

0 1 2 3

1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0

Klartext / Plain text: d i e s e ü n t e r s ü c h u n g b a s i e r t a u f d e m

Geheimtext / Cipher text: 52 55 25 72 25 22 95 08 25 86 72 22 67 72 22 95 31 42 13 72 55 25 86 08 13 22 14 92 26 83 11

Klartext / Plain text: p r i n z i p ① w e l c h e a l l g e m e i n a l s d a s

Geheimtext / Cipher text: 64 86 55 95 39 55 64 72 72 25 43 67 72 25 72 13 43 43 31 26 83 25 55 95 13 43 72 92 13 72 b

c d d.d.

Klartext / Plain text: r e l a t i v i t a e t s p r i n z i p b e z e i c h n e t

Geheimtext / Cipher text: 26 25 49 13 08 55 53 55 08 13 25 08 72 64 86 55 95 39 55 64 72 25 39 25 55 67 72 95 22 08 c

e f

Klartext / Plain text: w i r d ① w e l c h e s a b e r n i r g e n d w e l c h

Geheimtext / Cipher text: 77 55 86 92 24 72 25 43 67 72 25 72 13 42 25 86 83 55 08 55 67 31 25 95 92 72 25 43 67 72 d

b d. b.d. b.d.

Klartext / Plain text: e i n r e l a t i v i s m ü s s i c h t s t ü t ü n k a t ①

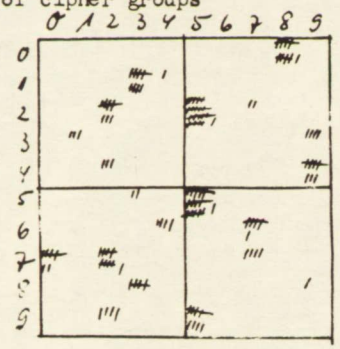
Geheimtext / Cipher text: 25 83 26 25 49 13 08 55 53 55 72 13 22 72 95 55 67 72 08 72 39 22 08 22 35 72 13 25 83 e

c

149 groups
= 149 Gruppen

Striche-Statistik der Geheimgruppen

Count of cipher groups



IA2

IA2 - 1

~~TOP SECRET~~

Doc ID: 6592461

Einfacher Fallcäsar, unsystematisch (27 Br)

Klarelemente Plain elements	a b c d e f g h i j k l m n o p q r s t u v w x y z ⊙ ⊙
Geheimelemente Cipher elements	13 42 67 92 25 14 31 70 55 05 80 49 83 95 16 64 38 86 72 08 22 53 77 20 97 39 89 27

Zweistellige Kettenstatistik
Count of successive dinomes.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	Belegung Frequency
08	25a.	12a.	55a.	13c.	72c.	72c.	55d.	72a.	22a.	83e.	55e					11 ✓
13	72a.	25a.	42b.	42b.	72d.	08c.	25c.	42d.	08e.	08e.						10 ✓
14	92a.															1 ✓
22	55a.	64a.	55a.	14a.	72c.	08c.	55c.									7 ✓
25	72a.	22c.	86a.	86a.	83a.	42b.	72d.	83b.	55b.	42c.	08c.	39c.	55a.	08e.	42d.	21 ✓
	12d.	86d.	55d.	42d.	83c.	42e.										
27	77b.	77d.														2 ✓
31	42a.	25b.	25d.													3 ✓
39	55b.	25c.	22c.	42e.												4 ✓
42	13a.	22a.	86d.													3 ✓
49	67b.	42b.	31b.	72b.	13c.	64d.	64d.	13e.								8 ✓
53	22a.	22c.														2 ✓
55	25a.	22a.	95b.	64b.	95b.	53c.	08c.	55c.	67c.	67c.	86d.	08d.	86d.	83e.	72e.	16 ✓
	67e.															
64	86b.	27b.	76c.	42c.												4 ✓
67	70a.	70b.	77c.	77d.	42d.	72e.										6 ✓
70	22a.	25b.	95c.	25d.	25d.	08e.	13e.									7 ✓
72	25c.	22a.	55a.	13b.	92b.	86b.	67c.	13d.	83e.	55e.	39e.					11 ✓
77	25b.	55d.	25d.	55e.												4 ✓
83	64a.	25b.	83d.	86e.	22e.											5 ✓
86	72a.	08a.	55b.	25c.	55c.	92d.	83d.	31d.	25e.							9 ✓
89	22a.															1 ✓
92	55a.	25a.	13b.	22d.	77d.											5 ✓
95	08a.	31a.	39b.	13b.	39c.	25c.	22d.	55e.	70e.							9 ✓

Geheimgruppen nach Häufigkeit geordnet
Cipher groups in order of frequency

20 groups

Geheimgruppen Cipher groups	25 55 08 72 13 95 86 49 22 70 67 83 92 39 64 77 31 42 27 53 14 85 = 22 Gruppen
Häufigkeit Frequency	21 16 11 11 10 9 9 8 7 7 6 5 5 4 4 4 3 3 2 2 1 1
Klartextentsprechung Plain equivalent	e i t s a n r l ü h c m d z p v g b ⊙ w f ⊙

Parallelstellen
Parallel passages

Geheimtext Cipher text	Stellung Position	Länge Length	Abstand Interval
64 86 55 95 35 55 64	b/1. c/14	14 = 2 . 7	86 = 2 . 43
27 77 25 49 64 70 25 72 13	b/8. d/5.	18 = 2 . 3 . 3	114 = 2 . 3 . 19
72 25 49 64 70	b/9. d/6. d/26.	10 = 2 . 5	154 = 2 . 7 . 11 40 = 2 . 2 . 2 . 5
86 25 49 13 [illegible]	c/1. e/3.	16 = 2 . 2 . 2 . 2	124 = 2 . 2 . 31

I A 2 - 2

3. Digit substitution with variants. (Mehrfach belegter Zahlencäsar)

Since the dinome substitution with its hundred possible cipher groups entails a possibility of additional values, it is natural that a further development was aimed at providing the most frequent plain elements with more than one cipher group. In the example in Appendix I A 3 a the substitution contains three groups each for plain e and i and two groups for plain s. The substitution itself is systematic in structure from two points of view:

1. The groups used lie only on definite diagonals in the number square (sheet 1 of the Appendix) and
2. The plain elements are entered first in the sequence of the letters of a key word (if letters occur more than once in the key word only the first occurrence is taken into account) and the remaining letters then follow in alphabetic sequence.

For purposes of analysis a 2-place chain count, shown on sheet 2 is prepared after determining the substitution elements by a group count. Due to the variants for frequent elements the count shows

1. An equalized frequency without prominent peaks, and
2. An increased number of cipher elements namely 25 different cipher groups for a text of 149 letters, in contrast to the previous average of about 20.

The interpretation of the cipher text on the basis of natural linguistic frequency would therefore run into difficulties. Consequently the count must be supplemented by an evaluation of the parallel passages. The superimposition of parallel passages on sheet 3 of the appendix shows that there are no relatively long continous parallel passages present, but only a number of relatively short passages following one another, and interrupted by one group which varies. Closer examination of the passages in position b 6 and e 2 (row and column index of sheet 1), namely the passages

11 88 22 93 28 58 11 52 03 06 58

52 88 22 99 28 58 11 93 03 06 88,

shows the interrupting groups are 93 coupled with 99 and 93 coupled with 52.

Since the parallel passages in position a 30 and c 14:

41 00 25 85 52 33 11 22 22

17 00 25 85 99 33 11 88 71

show interruption by cipher groups 52 and 99, it is natural to assume that 93 = 99 = 52 and that we have variants. This assumption is supported by the fact that the other parallel passages are likewise interrupted by dinomes which recur. If the variants are thus reduced so that instead of the three different dinomes 52, 93, and 99 we always enter the least dinome 52 in the cipher text, it appears

1. That interruptions of the parallel passages now disappear and
2. That new parallel passages appear, which could not previously be recognized, e.g. in position a 9, a 18 and d 28:

Reduced text: 52 00 52

Cipher text: 93 71 30, 93 00 30, 52 00 30

or in Position b 21 and c 11:

Reduced text: 17 17 17

Cipher text: 55 88 39 17, 55 41 39 88,

with which we may regard the hypothesis of variants as proved, especially since the cipher groups arranged according to frequency after their reduction (see sheet 2 of the appendix) reveal both a normal frequency curve and a number of different cipher groups corresponding to that of a simple substitution.

With proper evaluation of parallel passages the use of variants affords no protection against solution of the system; all that has been achieved is that the minimum amount of traffic required for solution is somewhat greater because short texts do not always provide for the parallel passages requisite for the reduction of variants or, to put it differently, interpretation of elements assigned more than one group calls for somewhat more cipher text. Assuming that there are enough variants and - and this is still more important - that full use is made of them in enciphering, this system can offer some degree of security when transmitting a short message.

Full utilization of the advantages of variants is quite difficult in practice since both the frequency peaks for the cipher elements must disappear and

parallel passages must no longer be recognizable as such. Here we have our first example of the fact that the theoretical security limit cannot be attained in practice, due to the difficulty of following out the rules for enciphering.

Consistent progress in the use of variants leads to full utilization of all the possibilities of the dinome substitution, namely the so-called hundred element substitution (Hundert-Elemente-Cäsar). Since this substitution may properly be used not merely to provide several variants for frequent plain elements but also to provide groups for frequent digraphs and trigraphs and frequent syllables, it is also called syllable substitution. (Silbencäsar)

In Appendix I A 3 b on sheet 2 are given the encipherment and decipherment tables for syllable substitution. It contains in detail:

15 letters	1 group each	15 groups
10 "	2 groups each	20 groups
1 letter	3 " "	3 "
3 Umlauts		3 "
2 marks of punctuation		2 groups
29 digraphs	1 group each	29 "
3 "	2 groups each	6 "
22 syllables, articles and words		22 "
	Total	100 groups

In the sample text on Sheet 1 of the Appendix the parallel passages of the plain text have been designated in the same manner. Comparison with the cipher text shows that these plain text repetitions can no longer appear as parallel passages in the cipher text if proper care is taken in enciphering and if the cipher text does not exceed a certain length.

On sheet 3 of the appendix is a 2-place group count of the cipher text. The arrangement of the cipher groups according to their frequency below shows a well equalized picture. Since frequency peaks and all recognizable parallel passages have dropped out, the system can be regarded as secure for single messages of limited length, if proper care is taken in enciphering the text.

But as soon as the text attains a length which no longer makes it possible

to avoid parallel passages in the cipher text or as soon as frequency peaks appear which give clues for attempts at decipherment, the syllable substitution looses all security because the entire system is readily solved once the first break has been made.

Doc ID: 6592461

Plain text
Klartext
Reduction
Reduktion
Geheimtext
Cipher text

1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0

das recht ist eine geistige und eine

39 33 71 28 17 03 06 30 93 71 30 17 52 63 17 42 88 93 00 30 93 47 28 14 63 39 17 52 63 41

Klartext
Reduktion
Geheimtext

sozialer wirklichkeit ist jede geisti

00 25 85 52 33 11 88 22 93 28 88 11 52 03 06 22 71 93 30 96 35 88 39 17 47 17 93 71 30 93

Klartext
Reduktion
Geheimtext

ger krise und jede soziale epoche

47 41 88 28 93 00 41 17 63 35 55 41 39 88 00 25 85 93 33 11 88 71 30 25 41 28 14 63 47 22

Klartext
Reduktion
Geheimtext

wirken sich auf das recht aus das ist

52 28 58 17 63 71 93 03 06 33 14 44 39 33 00 28 41 03 06 30 33 00 96 39 33 71 52 00 30

Klartext
Reduktion
Geheimtext

die wirkliche lage spiegelt krise

39 52 88 22 93 28 58 11 93 03 06 88 11 33 47 41 00 17 93 30 35 88 28 58 28 95 71 41 96

149 groups
= 149 groups

IA3a

Cäsarableitung mittels Schlüsselwort

Derivation of cipher alphabet by a key word

	0	1	2	3	4	5	6	7	8	9
0	s		c				h			
1		l			ü			e		
2			w				o		r	
3	t			a				b		d
4		e			f				g	
5			i				j		k	
6	m			n			p			q
7		s			v			x		
8			y				ä			ö
9				i		⊙				ü

Gruppenstatistik zur Feststellung der Geheimgruppen.

Group count to determine the cipher groups

	0	1	2	3	4	5	6	7	8	9
0	X			X			X			
1		X			X			X		
2			X			X			X	
3	X			X						X
4		X			X			X		
5			X			X		X		
6				X						
7		X								
8						X		X		
9				X			X			X

IA 3 a - 1

— 1 —

Doc ID: 6592461

~~TOP SECRET~~

Mehrfach belegter Zahlencäsar (22 Br)

Plainelements / Plain elements	a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	⊙
Geheimelemente / Cipher elements	33	36	03	35	17	41	00	41	44	06	22	93	99	55	58	11	66	63	25	66	69	28	00	11	30	14	44	22	77	82	85	96

Zweistellige Kettenstatistik des Geheimtextes
Count of successive dinomes

	1	2	3	4	5	6	7	8	9	10	Frequency Belegung	Frequency after reduction Belegung nach Reduktion
00	30a.	25b.	41c.	25e.	28d.	96d.	30d.	17e.			8	15
03	06a.	06b.	06d.	06d.	06e.						5	5
06	30a.	58b.	33d.	30d.	88e.						5	5
11	88b.	52b.	88c.	93e.	33e.						5	5
14	63a.	63c.	63c.	44d.	00d.						5	5
17	03c.	52a.	47a.	52a.	47b.	33d.	63d.	55e.			8	26
22	93b.	52b.	55e.								3	3
25	85b.	85c.	41c.								3	3
28	17a.	58b.	99c.	17c.	58d.	41d.	58e.	58e.	99e.		9	9
30	93a.	17a.	99a.	66b.	99b.	25c.	33d.	03d.	33e.		9	9
33	71a.	11b.	11c.	17d.	00d.	17d.	71d.	17e.			8	8
39	33a.	17a.	17b.	55c.	88c.	33d.	33d.	52d.	88e.		9	9
41	00a.	33b.	58c.	17c.	39c.	28c.	03d.	00e.	96e.		9	—
44	39d.										1	1
47	88a.	88a.	17b.	41c.	22c.	41e.					6	6
52	63a.	63a.	33b.	03b.	28d.	00d.	88e.				7	7
55	88b.	41c.									2	2
58	11b.	41b.	28c.	17d.	11e.	28e.					6	6
63	17a.	39c.	41c.	39c.	47c.	71d.					6	6
66	21	28a.	30a.	30b.	30c.	93d.	52d.	41e.			7	—
69	85	52b.	99c.								2	2
74	88	93a.	14a.	22b.	33b.	00c.	71c.	22e.	11e.	28e.	9	—
77	53	71a.	00a.	28b.	30b.	11b.	03e.				6	—
82	96	55b.	33d.	—e.							3	3
85	99	47a.	47b.	00c.	33c.	03d.	28e.	30e.	11e.		8	—

Cipher elements in order of frequency
Geheimelemente nach Häufigkeit geordnet:

1) vor Reduktion der Mehrfachbelegung
1) Before reduction of the variants

Geheimelemente / Cipher elements: 17 28 30 35 41 00 33 88 99 52 71 47 58 63 93 03 06 11 14 22 25 96 55 85 44 = 25 Gruppen (25 groups)

Häufigkeit / Frequency: 9 9 9 9 9 8 8 8 8 7 7 6 6 6 6 5 5 5 3 3 3 2 2 1

2) nach Reduktion der Mehrfachbelegung
2) After reduction of the variants

Geheimelemente / Cipher elements: 17 52 00 28 30 35 33 47 58 63 03 06 11 14 22 25 96 55 85 44 = 20 Gruppen (20 groups)

Häufigkeit / Frequency: 26 21 15 9 9 9 8 6 6 6 5 5 5 3 3 3 2 2 1

Äquivalente / Equivalents:

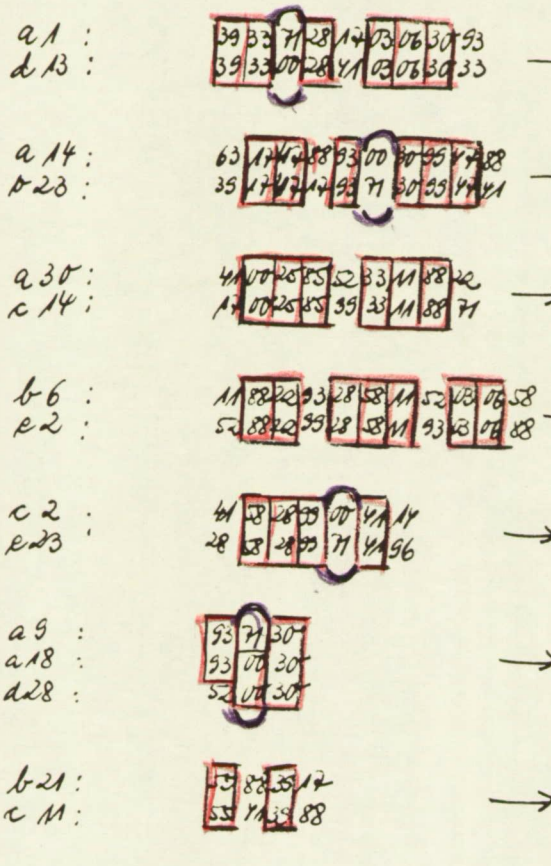
I A 3 a -2 -

— 2 —

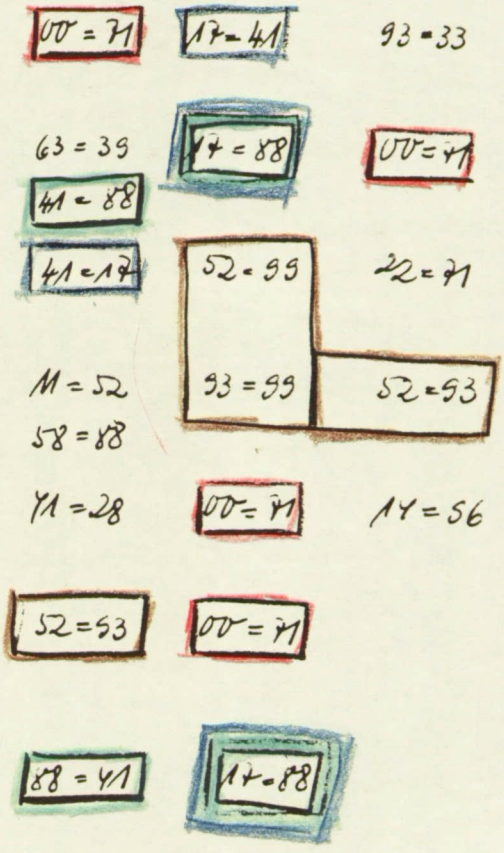
~~TOP SECRET~~

Doc ID: 6592461

Parallel passages = repeats
Parallelstellen:



Possible deductions
Mögliche Folgerungen



Bestätigte Folgerungen
Deductions confirmed

00 = 71
17 = 41 = 88
52 = 93 = 99

IA 3 a - 3

Doc ID: 6592461

TOP SECRET

1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0

Klartext / Plain text: Einem unserer Leser will es nicht gefallen, dass wir die

Geheimtext / Cipher text: 12 96 93 44 89 03 05 03 63 98 83 62 82 00 13 54 83 37 30 87 36 76 67 03 55 65 56 73 89 15 (a

Klartext: drei Aussenminister auf der Brüsseler Konferenz ein-

Geheimtext: 23 56 61 43 33 52 70 45 44 71 63 49 18 18 13 86 37 81 12 06 43 46 05 14 36 27 71 88 60 29 b

Klartext: ander Schlächelnd haben photographieren lassen. Er findet

Geheimtext: 38 34 78 16 48 42 53 87 19 57 50 05 54 56 73 79 86 13 35 64 44 69 03 71 57 32 50 19 32 05 c

Klartext: ihr Lächeln gezwungen und einer so ernsten Situation

Geheimtext: 15 00 87 25 93 68 28 12 63 22 86 18 52 37 87 66 10 53 16 41 77 38 82 06 00 33 56 32 79 70 d

Klartext: nicht angemessen. Überhaupt, meint er vorwurfsvoll, sei

Geheimtext: 25 92 60 94 87 66 52 53 35 16 63 07 25 10 03 13 31 75 78 83 52 44 58 62 20 11 54 33 92 58 e

Klartext: es bei den Amerikanern üblich, auf jedem Acker ein Lächeln.

Geheimtext: 43 06 86 15 70 33 71 02 61 78 27 64 87 72 72 66 48 87 94 05 59 24 36 32 05 28 79 f

285 Klardemente
285 plain elements

IA3b

I A 3 b -1

- 1 -

TOP SECRET

Doc ID: 6592461

Verschlüsselungstafel für Silbencäsar (27,100 Br)

Encipherment table

a	54	des	85	ge	00	l	71	q	99	ü	94
a	59	die	76	gen	68	ll	83	r	03	ün	93
ä	14	e	27	gr	42	m	31	r	92	ünd	28
an	06	e	32	h	19	me	53	re	80	v	75
aü	65	ei	55	h	72	mi	89	ren	90	ver	26
auf	61	ein	12	ha	60	n	15	s	45	vor	04
b	33	em	96	i	41	n	18	s	31	w	25
be	29	en	37	i	58	n	38	sch	21	wi	32
bei	20	en	73	ich	02	nd	88	se	44	x	02
c	50	er	63	ie	57	ne	40	si	84	y	07
ch	36	er	86	ih	69	nicht	82	so	22	z	87
d	67	es	09	im	95	nn	57	ss	56	aü	46
das	17	es	62	in	39	o	48	st	52	ü	70
dass	30	et	24	ist	23	o	77	t	16	⊙	79
dem	64	eü	47	j	78	ö	74	t	66	⊖	97
den	11	f	13	k	49	p	87	te	35	—	
der	43	g	01	l	05	ph	34	ü	10	—	

Entschlüsselungstafel für Silbencäsar

Decipherment table

	0	1	2	3	4	5	6	7	8	9
0	ge	g	ich	r	y	l	an	vor	x	es
1	ü	den	ein	f	ä	n	t	das	n	h
2	bei	sch	so	ist	et	w	der	e	ünd	be
3	dass	m	e	b	ph	te	ch	en	n	in
4	ne	i	gr	der	se	s	aü	eü	o	k
5	c	ie	st	me	a	ei	ss	nn	i	a
6	ha	auf	es	er	dem	aü	t	d	gen	ih
7	ü	l	h	en	ö	v	die	o	j	⊙
8	re	z	nicht	ll	si	des	er	p	nd	mi
9	ren	s	r	ün	ü	im	em	⊖	vi	q

1 A 3 b - 2

Doc ID: 6592461

Tvåställiga Gruppenstatistik des Geheimtextes.
Count of successive dinomes

	0	1	2	3	4	5	6	7	8	9
0	a d d		f f	a e		a b c c f f	b d f	e		a
1	d e	e	a b d	a b c e	b	a d f	c d e		b d	c c
2	e		d	b	c	d e		b f f	d	b e
3	a		c c f	b f	c		a b f	a b d d	c d f	c e
4		d	c	b b	a b e	b	b		b c c f	b f
5	c	c	d	d e e	a c c e	a	a c d		e e	c d f
6	b e	b f	a e	a b d e	f	a	d e f	a c	d	c
7	b d f	b b c f	f	a c		e	a	d e f	f	c d f
8	a	b d f	a d	a a e	a d		b b c d f	c e f	b	a
9	c	e	b e e	a d	e f		a	e e	a	

Letters in the cells refer to rows of page 1.

Chiffergruppen nach Häufigkeit geordnet:
Cipher groups in order of frequency

Chiffergruppe Cipher groups	05	86	03	13	37	48	57	63	71	00	06	12	15	16	27	32	36	38	44	53	58	59	66	70	77	79	87	93	87	52	usw.
Häufigkeit Frequency	6	5	4	4	4	4	4	4	4	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	
Klartextentsprechung Plain equivalent	l	er	r	f	en	o	a	er	l	ge	a	n	i	n	t	e	e	ch	n	se	m	ss	a	t	ü	s	o	Ö	z	ll	p	r

I A 3 b - 3

4. Digraphic substitution (Der Paarcäsar).

The striving for greater security led to the attempt to start not with a single element but with a digraph and to replace plain digraphs by cipher digraphs. In Appendix I A 4 a sheet 1 an encipherment table has been developed for this digraphic system, with a decipherment table on sheet 2. This system is called the Deutscher Paarcäsar (German digraphic system).

On sheet 2 of the appendix a plain text had been enciphered with this. The repeated digraphs and parallel passages disclosed by the digraphic count on sheet 2 have been marked and provided with appropiate line indices pointing to the preceding and following occurrences of the same passage. A comparison of the parallel passages appearing in the plain text with those appearing in the cipher text shows that the parallel passages of the plain text appear in the cipher text only when they stand at an interval of 2 or a multiple thereof or - to state it in more general terms - when they are in "phase".

To explain the concept "phase" (Phase) it is necessary to explain first the concept "period" (Periode). As the period of a system we designate the least interval after which a genuine parallel passage may reappear in the cipher text. A repetition in the cipher text is termed a genuine parallel passage when the repetition in the cipher text and the plain text correspond to one another. Two passages are then considered to be in phase when they occupy the same position within the period.

In the present case two passages of text are in phase when they stand at an interval of two or a multiple of two. Moreover plain text repetitions appear as parallel passages in their full length only when they extend from the beginning of the period to the end of another period. On the other hand the first and last element will not appear in the parallel passage if it extends beyond the beginning or the end of a period.

With this system we meet for the first time the phenomenon that cipher text repetitions do not always indicate plain text repetitions as was the case with all simple letter substitutions. In line 6 column 26 to 30 the cipher text

ua ua does, to be sure correspond in the plain text to a digraphic repeat ne ne; on the other hand in line 1 column 12 to 15 and line 2 column 4 to 7 the repeated digraphs yn yn and yc yc respectively do not correspond to repeated digraphs in the plain text because the first and last elements of the parallel passages always extend into two different periods. This likewise explains the earlier remark that cipher text repetitions are only to be regarded as parallel passages when they are of a definite minimum length depending on the system and the amount of traffic. This minimum length must be so chosen that the parallel passages to be utilized will all or at least predominantly be genuine parallel passages.

Since in the present example the number of parallel passages - two textual repetitions each 10 elements long - does not suffice to determine regularities in the length and interval of parallel passages with any certainty, it is necessary to resort to digraphs. There is no objection to doing this if one is aware of the extent to which digraphic repeats may represent false parallel passages, so that corresponding deductions will be drawn only from the average or the majority of all results so as to avoid reaching false deductions as a result of evaluating false parallel passages.

Information regarding the ratio of genuine parallel passages to false parallel passages in our present example is afforded by a comparison of the two counts on sheet 3 with the chain count on sheet 2. A study of the total of 120 repeated cipher digrams occurring in the present example shows that 71 digraphic repetitions extend from the beginning of the period to the end of the period while 49 repetitions run from the end of one period to the beginning of a second period.

Thus the first 71 digraphs represent genuine parallel passages while the remaining 49, insofar as digraphs are not concerned which stand within genuine parallel passages, are not genuine parallel passages.

Now if the number of intervals is checked which can be derived from these digraphs, it appears that

1. The 71 digraphs yield 74 intervals among themselves all of which are even numbers;
2. The 49 digraphs, although they are not genuine parallel passages, yield 30 intervals which are likewise even numbers;
3. The 71 digraphs and the 49 digraphs together also yield only 23 intervals which are odd numbers.

Since between the 120 digraph repeats there are a total of 127 intervals, of which 104 are even, the correct result stands out so sharply that the study may be extended to include all digraphic repeats.

On sheet 2 of the Appendix the lengths and intervals of the parallel passages, including repeated digraphs, are broken up into their least factors and the number 2 has been recognized as a common factor.

The analysis of the German digraphic substitution shows then the following characteristics:

1. No linguistic frequency of the single elements of the cipher texts.
2. The number of parallel passages including all repeated digraphs corresponds on the average to half the linguistic frequency.
3. The parallel passages in their length and intervals show the number 2 as a common factor.

   Their length, depending on the position in the text, may be as much as two elements shorter than the corresponding repetitions in the plain text.

Consequently it may be stated that the security of the German digraphic substitution is greater than that of any simple substitution. Nevertheless the German digraphic substitution can be used only within very narrow limits if its security is to be maintained. With a certain amount of material interpretation based on digraphic repeats and the frequency of plain text digraphs is no more difficult than the interpretation of the simple substitution. The amount of material will hardly exceed one to two pages of text.

Doc ID: 6592461

In practice, therefore a new digraphic substitution should be set up for every message of medium length. As experience shows, the time required for this is considerable because there are numerous sources of error both in setting up the encipherment table and setting up the corresponding decipherment table. The time expended in producing cryptographic material is, therefore, in no proper ratio to the possibilities of use.

In this respect a similar method, namely the English digraphic substitution (Playfair cipher), has great advantages over the German method, because the production of cryptographic material is very simple and requires only a few seconds.

For enciphering and deciphering, a square with 5 x 5 = 25 cells is used in which the letters of the alphabet without j (which is always replaced by i) are entered in any desired sequence. Encipherment follows these rules:

1. If the two plain elements to be enciphered stand in a horizontal row of the square, the letters standing to the right of the plain elements are selected in the same order as cipher elements. The first letter at the left end of the row is considered to be the letter at the right of the one at the right end of the row.

2. If both the plain elements are in one column the letters standing below them are taken as cipher elements. The top letter of the column is considered to be the letter below the lowest letter.

3. If the two plain elements to be enciphered are in different rows and columns then the cipher elements are those letters which with the plain elements form the corners of a rectangle. The letter above or below the first plain element is regarded as the first cipher element.

If the square has the 25 letters of the alphabet in the sequence;

a b c d e
f g h i k
l m n o p
q r s t u
v w x y z

then according to the rules: plain ab = cipher bc, plain ad = cipher be,
plain ae = cipher ba, plain af = cipher fl, plain al = cipher fq,
plain av = cipher fa, plain ag = cipher fb,
plain ar = cipher qb and plain lz = cipher vp etc.
The same rules, appropriately modified, apply in deciphering.

Since according to these rules a doublet, i.e. a digraph consisting of two like letters, cannot be enciphered by the square, it is necessary to doctor the plain text of Appendix 1 A 4 b before encipherment in such fashion that doublets, if they do not divide between two periods, be separated by inserting an x.

Analysis of the cipher text yields the same results as with the German digraphic substitution. However other phenomena occur due to the fact that the English digraphic substitution shows a systematic character due to the use of the cipher square. As the presentation on sheet 3 of the Appendix endeavors to show, this structure causes

1. That only 600 different digraphs are possible in contrast to 676 digraphs of the German digraphic substitution, because the alphabet contains only 25 letters and doublets drop out as digraphs;
2. That of the 600 digraphs all those which do not lie in the same row or in the same column of the square, i.e. 400 digraphs, are reciprocal and reversable.

   I.e. if

   plain ab = cipher ur, then the reverse

   plain ba = cipher ru, is correct. Furthermore,

   due to the reciprocity, we also find

   plain ur = cipher ab and

   plain ru = cipher ba. Hence if one of these 400 digraphs is interpreted, 3 others follow automatically;
3. That the remaining 200 digraphs formed of letters in the same row or in the same column are reversable; hence

   plain be = cipher ub, and

   plain eb = cipher bu.

Hence in this case each interpretation yields 2 digraphs. Consequently only 200 digraphs need be interpreted in contrast to 676 of the German system.

Furthermore the regularity inherent in the English digraphic substitution permits the reconstruction of the cipher square on the basis of a few interpretations. Such a reconstruction of the square has been made on sheet 4 of the appendix by the aid of 17 digraphs which are assumed to be known. In this example it follows from equation 1:

Plain be = cipher ub, that these three elements are either located under one another in the colomn as b (u / e) or side by side in the row as e b u. From equations 2 and 3 we also get two possibilities each. Since the third equation cuts into the first two in one letter in each case,

we get a grouping of these equations as

u		s g h
s b	or	e b u
g e v		v
h		

From equation 4 it appears that only the second form is compatible with this equation so that we have as correct fragment of the square

s g h
e b u k
v

In this fashion the square can be further developed with each new equation as following the colored markings in the Appendix clearly shows until we have it

s g h z o
p e b u k
v m i c
f q d t n
y l r a w

Since only the letter x remains for the vacant cell this can be supplied. This square represents a displacement of the original square toward the top and side; its effect is the same.

In summing up we may say that the English digraphic substitution has some advantages over the German digraphic substitution in the preparation of cryptographic material but that the characteristics of the square result in far less security so that material enciphered with the English square must be kept less, if the same degree of security is to be maintained.

Doc ID: 6592461

TOP SECRET

TOP SECRET

Versätzerungstafel zum Schlüssel Saarcäsar (2BBr)

Enciphering table

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	ma	bæ	go	væ	rl	ük	jd	ca	bü	ve	rb	br	so	rw	di	vf	wl	kt	sæ	æz	go	sc	ag	mw	yj	rr
B	üb	pc	lf	bg	pa	cü	æz	zj	sf	so	mr	tz	yg	ll	av	gu	me	di	dk	nd	nü	zg	dd	v	kc	gu
C	dk	ca	oe	æz	m	br	kd	lk	æ	n	yr	æz	æ	æ	nü	r	n	b	r	gk	m	ra	br	if		
D	æw	lf																								
E																										
F																										
G																										
H																										
I																										
J																										
K																										
L																										
M																										
N																										
O																										
P																										
Q																										
R																										
S																										
T																										
U																										
V																										
W																										
X																										
Y																										
Z																										

Appendix I A 4 a - 1

Doc ID: 6592461

TOP SECRET

Entzifferungstafel zum Deutschen Saarcäsar

Deciphering table

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	oi	hm	dp	lp	rg	hv	av	oy	hg	od	sb	ia	ce	xj	gv	xt	ss	kü	cz	sz	xx	zp	bv	ic	bc	ükt
B	gp	rh	nl	ch	hd	ob	bd	or	sh	ay	üt	üx	zl	cg	gj	mo	is	al	iz	gx	eü	kc	cm	ab	ii	rm
C	ah	of	kn	vp	xg	ro	ot	lv	tc	va	pc	ih	ic	dr	nv	bz	pv	sl	gh	di	tf	jc	dc	zl	uz	lk
D	fi	fo	üm	bv	qp	sj	lf	ca	ao	pl	bs	pt	cv	nv	xx	sü	vv	vn	üi	ij	el	xf	yy	rs	zl	zb
E	vb	sh	om	ip	by	lq	rm	pü	mi	my	zs	wv	hy	iv	ij	gf	jg	ld	ri	ükc	qj	tm	za	lt	xx	at
F	ov	sr	xo	zk	kc	db	dü	jm	jy	re	ra	pj	kr	vs	iv	ry	ok	pg	üf	vc	kf	fm	tg	to	ü	vt
G	gd	dg	lb	lo	pn	vl	üs	gt	ok	ez	fv	by	rh	bp	ac	bd	rc	ol	io	ls	hü	ck	zm	ri	vz	xv
H	xo	bq	xv	qr	nd	hk	ca	dk	nk	ds	do	b.	tp	gü	xv	lz	qx	kr	gl	gr	ii	na	oj	td	nb	kc
I	oo	ch	rk	mc	mv	cv	eg	fj	dk	ük	sf	ri	mr	lm	kc	gd	xe	rf	jk	fr	bü	üv	gt	ov	np	kj
J	ee	fp	cp	ag	eh	ki	le	si	mt	eü	ür	vv	mx	sg	gs	ps	mn	ve	il	sk	üj	yd	ds	üa	tq	fv
K	fg	rg	gb	zg	nk	gn	hk	zq	rr	üü	fx	op	vm	jt	ix	kv	ky	gt	fs	ar	ai	mq	id	fb	zh	vj
L	sk	sf	po	ko	hq	gj	if	gk	fa	oc	hm	fz	xp	zk	qv	st	kv	iq	xy	üy	rz	ok	nü	rl	nj	bq
M	aa	df	vk	xp	bg	bm	cj	kf	gi	tl	go	lr	ct	lk	nh	kd	ia	gk	tq	km	ht	tv	vv	ov	vp	qk
N	vc	ya	ge	kd	gs	pp	bü	dy	sz	yo	yx	vi	jl	nf	md	tb	pa	gi	kn	cq	ev	jv	fü	yq	üm	nt
O	rm	pf	nc	ff	cc	ap	rn	vv	py	yz	mü	ko	oj	vf	gv	sd	qk	ym	kq	xt	vx	hyk	üo	pr	ll	cl
P	be	hv	bb	jü	kq	yc	yp	rs	kx	ln	yü	vh	qa	vd	uě	gr	fk	pm	zq	sm	vq	kv	ny	jv	vm	üp
Q	tk	sk	qf	ta	vc	tr	bs	tn	xn	vi	rd	nb	ll	qq	on	jq	js	dv	nx	ik	lq	kb	ge	ti	ol	jo
R	cü	ak	rp	ml	fy	mv	mp	iq	fe	lc	dd	ae	ni	vl	ts	lü	gv	az	ty	tü	xt	cr	an	vo	gl	hym
S	vj	vg	qn	ls	av	bi	ke	jb	ed	xh	ms	kv	ax	dt	am	qq	lc	zb	ys	qs	ky	cq	bx	as	ej	kv
T	vü	so	dn	cg	dx	bc	ey	ie	vk	gc	vv	qx	pq	gj	ja	vn	yv	ws	tx	pi	ld	cf	rj	me	dm	bl
U	ne	ba	oj	im	eo	kl	dv	os	co	ki	af	yr	vü	kx	iv	tz	go	fl	ji	ke	vf	tb	tx	so	ng	jd
V	ka	uü	dq	yl	rü	ey	kn	ij	dc	tf	px	zq	cy	vv	yf	ep	mj	za	nd	yx	vt	ül	ci	ad	nf	ma
W	pd	gm	gü	bt	aj	ll	fd	bk	mm	kv	ga	az	zq	ms	wv	mq	jk	gk	uv	ps	jp	jx	pb	bg	lf	üd
X	vv	ir	üq	tj	kx	it	sv	dq	tr	bl	pk	mt	ki	dl	cn	ns	kx	fn	xx	gq	üb	bk	ef	pk	vr	xt
Y	tr	mo	da	zs	bm	xb	xx	yi	gy	yg	pe	lv	ex	de	aü	oa	kx	hp	sm	jk	tt	nx	sc	yv	ng	gb
Z	cb.	iy.	op.	li.	ft.	tx.	bv.	fq.	by.	ix.	pt.	xy.	jf.	xy.	ge.	jc.	ib.	se.	va.	sa.	fc.	xc.	jn.	cd	eq.	px

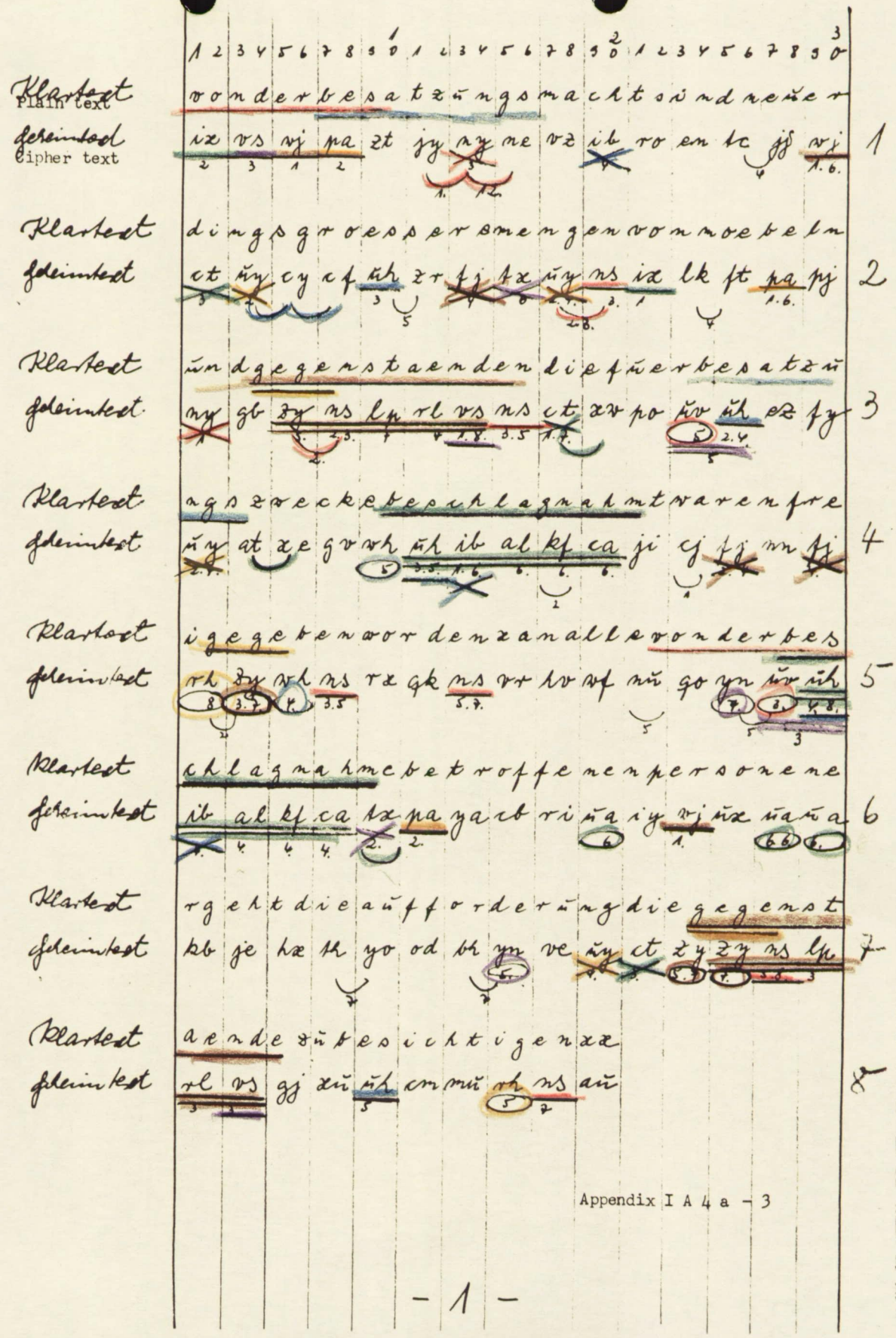
Appendix I A 4 a - 2

TOP SECRET

hh

Doc ID: 6592461

~~TOP SECRET~~



Appendix I A 4 a – 3

~~TOP SECRET~~

Doc ID: 6592461

~~TOP SECRET~~

Einstellige Kettenstatistik des Geheimtextes

Digraphic count of the cipher text.

	1 2 3 4 5 6 7 8 9 0 1 2	Frequency Häufigkeit
A		14
B		7
C		11
D		1
E		6
F		9
G		3
H		13
I		8
J		14
K		5
L		7
M		2
N		16
O		5
P		7
Q		2
R		9
S		10
T		10
U		18
V		10
W		6
X		10
Y		18
Z		8

Parallelstellen und Digramme

Parallel passages and repeated digraphs

Geheimtext Cipher text	Stellung Position	Länge Length	Abstand Interval
zynslprlvs	3/5. 7/25	10 = 2·5	140 = 2·2·5·7
ühibalkfca	4/11. 5/28	10 = 2·5	48 = 2·2·2·2·3
üvvük	3/23. 5/27	4 = 2·2	64 = 2·2·2·2·2·2
ns	2/13. 3/7. 3/15 5/7. 5/13. 7/24 8/14.	2 = 2	18 = 2·3·3 26 = 2·13 72 = 2·2·2·3·3 84 = 2·2·3·7 156 = 2·2·3·13 178 = 2·89
yn	~~1/12. 1/14. 2/12 2/18. 5/8. 7/15. 7/16.~~	2 = 2	50 = 2·5·5

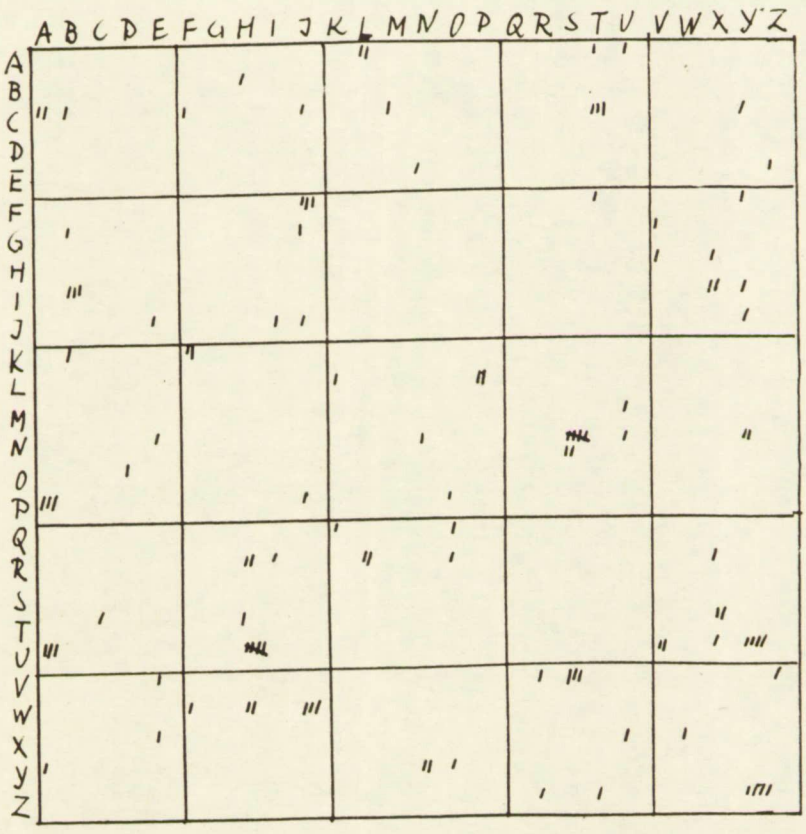
IA4a-4

~~TOP SECRET~~

Doc ID: 6592461

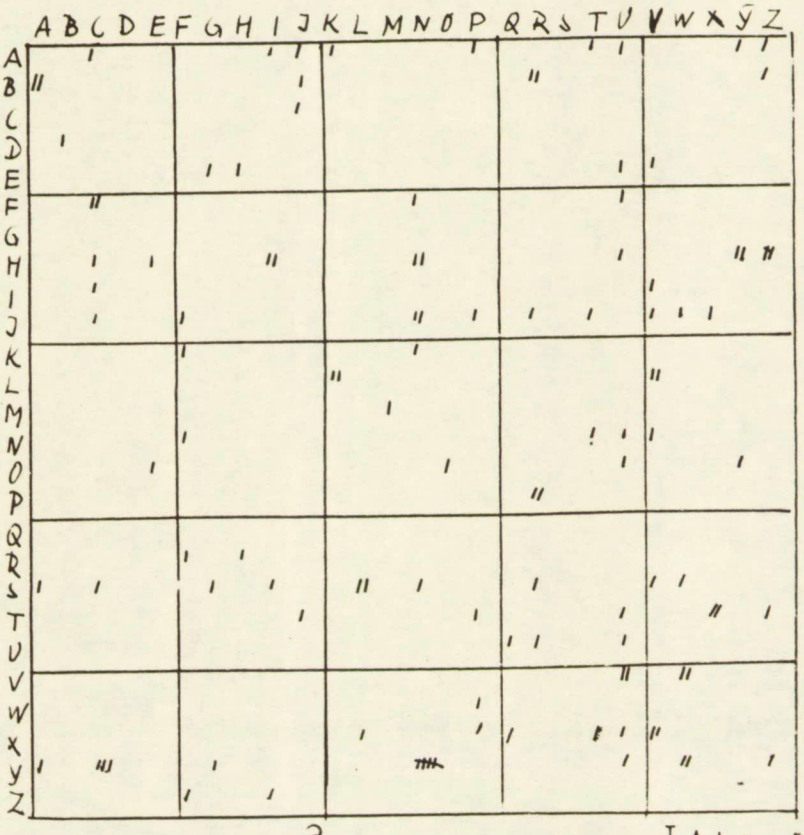
Zweistellige Gruppenstatistik in Phase.

Digraphic count in phase



Zweistellige Gruppenstatistik mit Verschiebungsgrad 1.

Digraphic count with slide of 1



Doc ID: 6592461

~~TOP SECRET~~

Klartext Plain text	vonderbefehlsübergabeamtsvorsteher	
Geheimtext Cipher text	gc ft lb üb yz aü tk hg ri om žf tc tf bk lb 2. 3. 1. 2. 3. 4. 1. 5.	1
Klartext	dingsgroessere mengen von moebeln	
Geheimtext	mt oq gh hv gp pg bl bv oq gk gc cd kg üb gv 3. 2. 6. 3. 4. 2. 4. 3. 1. 5. 1. 5.	2
Klartext	und gegenstaende die fuer beschlagnahmt	
Geheimtext	tk hg ve gk ps ül ft gk mt gp kb hm gp za üi 1. 7. 5. 2. 3. 1. 5. 3. 5. 2. 2. 4. 8.	3
Klartext	ngs zwecke beschlagnahmt waren fre	
Geheimtext	oq go kl nc bü gp om vv go dr di yv bl fq bl 2. 5. 3. 1. 8 2. 4. 4.	4
Klartext	igegebenworden x analoge vorderbe	
Geheimtext	zü ge bü gk ok hv gk yi vt vy go gc ft lb üb 3. 4. 6. 3. 5. 7. 5. 8 6. 2. 3. 1. 6. 2. 8.	5
Klartext	schlagnahme betroffenen personne	
Geheimtext	xo rg zl nt bd bü gü hv yf pq kg kf lb gs kg 5. 5. 2. 7. 6. 5. 7. 6. 7.	6
Klartext	nergehtdie aufforderungdiege	
Geheimtext	kg hl gb nt üv di yf sn hr lb tk gk üv ov ev 7. 7. 6. 5. 6. 3. 7. 7. 7. 8	7
Klartext	nstaendeübersichtigen x	
Geheimtext	of as gk bq üi üb zz om at ov cf 5. 3. 5. 4. 7.	8

IA4b

I A 4 b - 1

— 1 —

~~TOP SECRET~~

IA4b

Doc ID: 6592461

Englisher Paarcäsar (2 Br)

English digraphic substitution (Playfair)

b	ü	k	p	e
m	i	c	x	v
d	t	n	f	q
r	a	w	y	l
h	z	o	s	g

ük = kp = ükp →
kü = pk = pkü ←
it = ta = ita ↓
ti = at = ati ↑
ib = üm } iü same column or
bi = mü } bm row
üm = ib
mü = bi

Zweistellige Gruppenstatistik

Digraphic count

	1	2	3	4	5	6	7	8	9	10	11	Belegung
A	ü₁ z₂ t₃											3
B	k₁ l₂ v₂ ü₃ l₄ l₄ ü₅ d₆ ü₇ q₈											10
C	d₂ f₈											2
D	i₄											1
E	o₂ v₃ o₃											3
F	t₁ z₂ t₃ q₄ t₅											5
G	c₁ l₂ n₃ c₄ f₄ o₄ y₄ v₅ l₅ z₆ t₇											11
H	g₁ v₂ q₃ m₃ r₅ v₇ l₇ r₈											8
I												—
K	q₂ b₃ l₄ z₄ f₄ q₄ z₇											7
L	b₁ b₁ b₅ b₆ b₇											5
M	t₂ t₄											2
N	c₄ t₇											2
O	m₁ q₂ q₂ q₄ m k₆ f₈ m₈											8
P	q₂ q₆											2
Q	b₂ b₂ k₂ k₃ p₃ o₄ k₄ k₄ ü₆ l₄ k₈											11
R	i₁ v₄ q₆											3
S	n₇											1
T	k₃ c₁ f₁ k₂ k₈											5
U	b₁ b₂ l₃ i₃ t₅ v₆ v₃ i₂ b₃											9
V	e₂ e₅ y₅											3
W	t₅ t₆											2
X	o₆ z₈											2
Y	z₁ v₄ i₅ f₆ f₇											5
Z	f₁ a₃ r₄ b₅ l₆ i₇											6

Cipher text of parallel passages not in phase.

Gleichlaufende von nicht in Phase liegenden Klartext-parallelstellen:

Klartext: g e g e n s t a e n d e
Plain text

3/3: | l q | ü e | q k | p s | ü l | f t | q k |

11/24: | e ü e v | ü q | a z | q k | b q |

Klartext: b e s c h l a g n a h m
Plain text

4/5: | b ü | g p | k m | r w | q o | z r | i l |

5/25 | ü b | x o | r g | z l | r t | b d |

Klartext: b e s a t z ü n g s
Plain text

1/7: | ü b | j z a ü | t k | q z |

3/28: | l m | g p | z a | ü i | r q | q o |

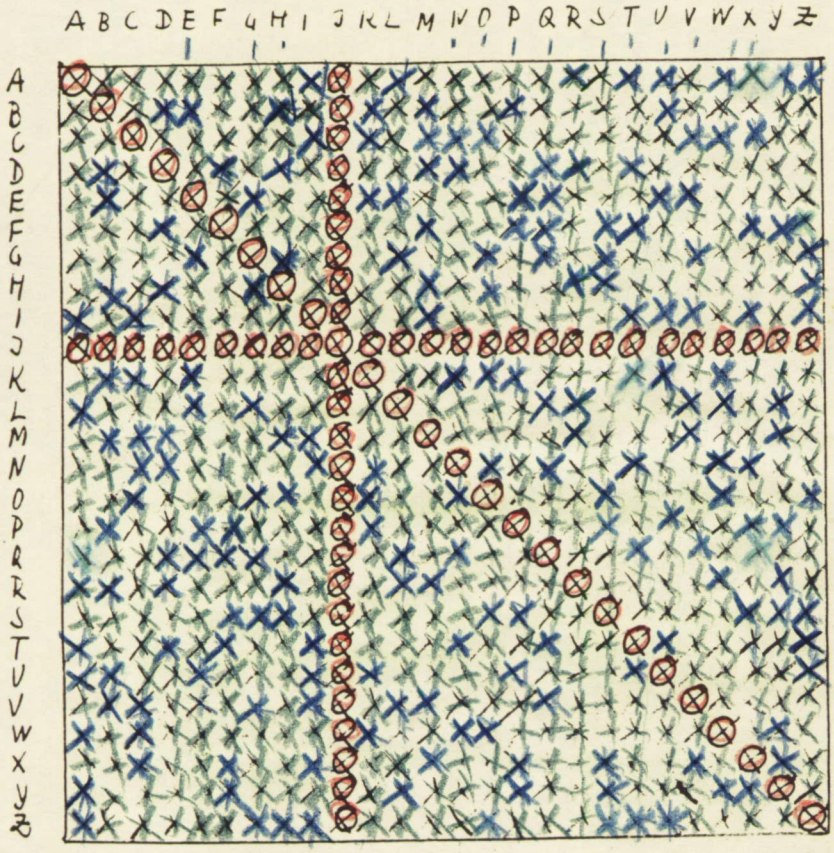
IA 4 b - 2

TOP SECRET

~~TOP SECRET~~

Belegung und Gesetzmässigkeiten des Englischen Playfair.

Possibilities and regularities of the Playfair.



76 ⊗ = Digramme nicht belegbar
digraphs which cannot occur

200 X = Digramme aus Buchstaben derselben Zeile oder Spalte
digraphs made up of letters from the same row or column.

400 X = Digramme aus Buchstaben verschiedener Zeilen und Spalten
digraphs made up of letters from different rows and columns.

Beispiel für X Digramm: Example of digraphs
bü = hk
üb = kü
= umkehrbar reversible

Beispiel für X Digramm: Example of digraphs
bg = he } umkehrbar
gb = eh } reversible
he = bg } umkehrbar
eh = gb } reversible
} reziprok reciprocal

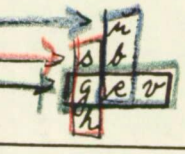
I A 4 b - 3

~~TOP SECRET~~

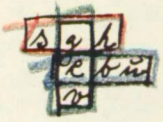
Doc ID: 6592461

Reduktion des gesamten Daarcäsars
Reduction of the entire substitution by the aid of a few solved digraphs.
mit Hilfe einiger gelöster Digramme.

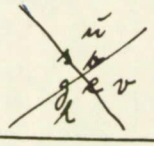
	Plain Klar	=	Cipher Geheim
1)	be	=	ŭb
2)	gs	=	hg
3)	kg	=	vk

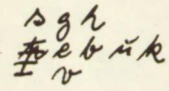


oder

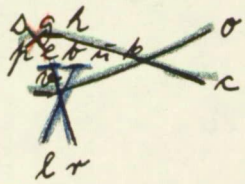


4)	eŭ	=	bk

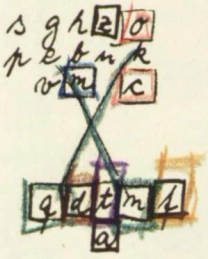




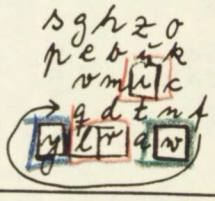
5)	es	=	gp
6)	er	=	lb
7)	vo	=	gc

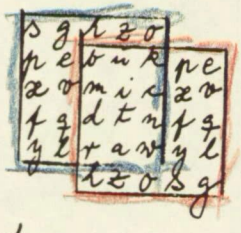


8)	ve	=	kg
9)	ch	=	om
10)	en	=	kq
11)	nm	=	cd
12)	ŭn	=	fk
13)	nd	=	ft
14)	tz	=	aŭ



15)	ma	=	ri
16)	sa	=	yz
17)	vo	=	lw





I A 4 b - 4

5. Substitution with nulls (Cäsar mit Blender).

The attempt described in Appendix I A 5 a to give the simple substitution greater security takes a different course. Here so-called nulls are introduced at optional positions in the cipher text, in this case the digits 4 and 9, which were not used for the substitution alphabet and which are left out of account when deciphering. As a result a dinome group count fails to yield a characteristic substitution picture (see the count on sheet 3 of the Appendix). Instead of the 2-place chain count used hitherto a 4-place displacement count (vierstellige Verschiebestatistik) (see sheet 2 of the appendix) must be undertaken in order to discover all the parallel passages. The 4-place displacement count, assuming a cipher text

0 1 2 3 4 5 6 7 8 9 1 2 3 4 etc., is made in such fashion that the following groups are counted one after the other: 0 1 2 3, 1 2 3 4, 2 3 4 5, 3 4 5 6 etc. If the designation of the lines of the count is 1-place, then the last three places of the group to be counted are entered on the line; if the line designation is 2-place, then only the last two places of the group are to be entered etc. (of course for the border line case where a 1-place letter system is involved as in the case of a simple letter substitution the 1-place chain count is like the 2-place displacement count.)

The parallel passages disclosed by this displacement count show various interruptions by single elements in the text at one point to which no other elements correspond at the point where the repeat occurs (see comparison of parallel passages on sheet 3 of the Appendix.)

The complete analysis of a substitution text with scattered nulls has the following characteristics:

1. The 2-place group count does not show alphabetic frequency.
2. The same group count with a displacement of 1, i.e. omitting the first element, gives a similar picture(sheet 3 top and center).
3. Common to both counts is the low score of certain columns, in this case columns 4 and 9.

Doc ID: 6592461

4. The displacement count shows up parallel passages with interruptions showing additional elements to which nothing corresponds in the counterpart.
5. The intervals between parallel passages are odd and even.
6. The length of the parallel passages, omitting the interruptions, is 2-place.

Careful evaluation of the parallel passages is important for the recognition of the mull. As soon as one suspects that a mull may be present, it is easy to find confirmation.

Besides this mull inserted at arbitrary places, the so-called wild mull (wilden Blender), there is the systematic mull (systematischen Blender). As its name suggests, this mull is inserted at definite, prearranged positions in the text. Since the position of the mull is fixed, any digits may be used for the purpose.

In Appendix I A 5 b is given an example of this procedure with a systematic mull in columns 5, 15, and 25. In contrast to the wild mull both parallel passages show interruptions and the position of the interruption in the parallel passage may vary. If two or more interruptions appear in parallel passages, the intervals between the interruptions will be the same. Their position within the parallel passage may be displaced with respect to one another.

In analysis the regular interval for all interruptions is the most important characteristic.

Since once a mull, whether wild or systematic, has been recognized, only a simple substitution remains, this device cannot be regarded as an effective improvement on the simple substitution.

Doc ID: 6592461

~~TOP SECRET~~

Klartext
Plain text

1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0

das passions spielkommitee hat tzwei 1
nen antrag auf wiederholung des pas 2
sions spiels abgelehnt zwei wiederho 3
lung soll durch abstimmung erre 4
icht werden 0 5

131 Elemente

Geheimtext
Cipher text

| | | |

Doc ID: 6592461

TOP SECRET

Dreistelliger Ballencäsar (23 Br)

Dinome substitution

Klarelemente / Plain text: u b c d e f g h i j k l m n o p q r s t ü v w x y z ö

Geheimelemente / Cipher text: 31 23 50 67 16 78 57 82 08 86 36 41 55 63/11 25 80 06 60 19 52 68 28 71 73 33 38

Unsystematische Blender 4 und 9

Random nulls = 4 and 9

Vierstellige Verschiebestatistik des Geheimtextes

4 digit displacement count of the cipher text

00 87a.87e.
1 42g.70h.
2 33a.50a.53b.55e.
3 42e.
4 60a.85h.82i.
5
6 02a.31c.98d.00e.02e.52g.57h.06i.16i. 67i.
7
8 11a.16a.17b.63c.16c.11e.16e.63f.16f.33h. 50i.
9
10
1 63a.55b.71b.21d.63e.64f.21g.21g
2 15d.35b.15g.12g.16g.26h.
3
4
5 50b.73c.27c.36d.26g.
6 02a.04a.36a.21a.16b.82b.16b.08b.63c.67d. 05d.60d.06e.39e.21e.83e.21f.48f.08f.28f. 67g.06g.75g.06i.08i.06i.63i.
7 16b.17b.11b.06c.38f.04h.28i.
8
9 36b.
20 65h.
1 93b.42d.52d.60e.16f.12g.52g.21g.67g.72i.
2
3 11b.59e.12h.60h
4
5 41a.08a.31d.08e
6 35d.31f.85g.35h.
7 62c.
8 08c.08f.16i.
9
30
1 60a.60a.17b.66c.63c.70c.57c.52c.60e.93e.73f. 62f.20h.
2
3 16c.
4
5 76d.71f.76g.71h.
6 06a.46b.07h.
7

38 16f
9 60e.
40
1 41b.
2
3
4
5
6 00a.
7
8 26f.55h.21i.
9
50 87a.87b.87e.82h.48i.
1
2 78c.63d.63g.06h.63h.
3 16a.16d.
4
5 08b.55h.55h.52h.36h.
6
7 31c.67d.16f.60g.46h.
8
9
60 45a.46a.08a.60a.25a.60b.06c.69d.25d.60e.08e 60e.25e.41a.86f.68g.11g.71h.60i.61i.55i. 66i.
1 15b.68b.60i
2 19b.16e.11f.50f.
3 60a.16c.31c.17c.15c.57d.36e.17f.16f.57g.57h. 38i.
4 82f.
5 08h.
6 33c.71d.02d.79g.71i.33i.
7 41a.16d.16d.31g.52g.16i.
8 23b.21g.
9 42d.
70 63c.48h.
1 41b.71b.60d.66d.64f.60h.66i.
2 87i.
3 16a.15c.87f.
4 16b.
5 20h.

76 71d.17g.
7
8 28c.
9 16g
80 87c.81f.
1 16a.62a.71b.66d.16e.62e.60f.66f.60i.
2 41b.50c.41d.63f.11g.71h.17i.
3
4
5 55h.04i.
6 31c.31f.
7
8
9
90
1 60g
2
3 41b.
4
5
6 06e.
7
8 21d.
9

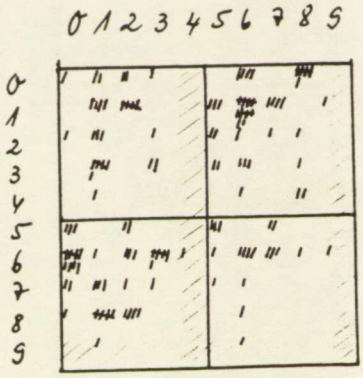
IA 5a - 2

— 2 —

Doc ID: 6592461

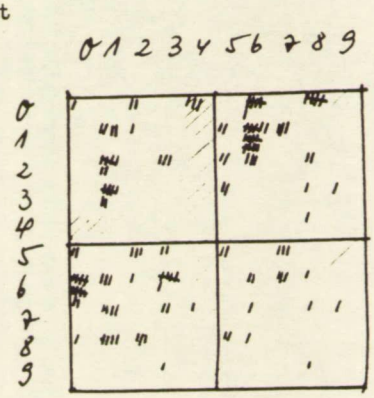
Dinome count

Zweistellige Strichelstatistik des Lyrenintextes



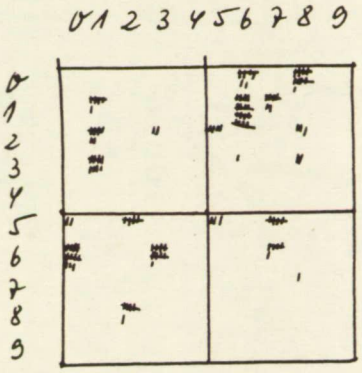
Dinome count omitting the first element

Zweistellige Strichelstatistik des Lyrenintextes unter Auslassung des 1. Elements



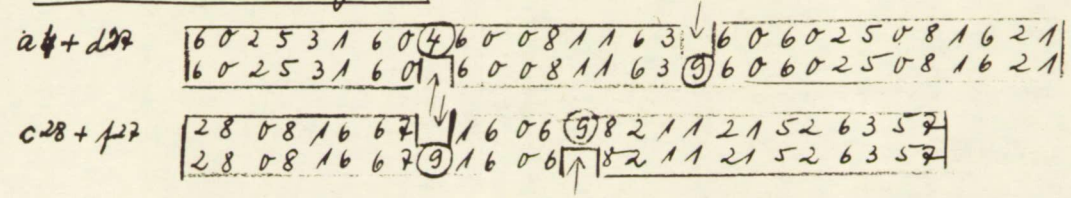
Dinome count omitting the nulls 4 and 9.

Zweistellige Strichelstatistik des Lyrenintextes unter Auslassung der Ziffern 4 und 9



Comparison of parallel passages.

Parallelstellenvergleich



Doc ID: 6592461

1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0

Klartext: die bayerische studentenzeitung i 1
Plain text

stdieeinzige studentenzeitungta 2

yernsOsiefuehrtalsbeilagediede 3

ütschestudentenzeitungO 4

113 Elemente
113 elements

Geheimtext
Cipher text

1 8 1 5 5 4 5 0 9 3 6 5 9 4 3 5 4 2 1 5 1 1 5 6 2 4 5 1 1 9 a
a.g. e. a.g.

9 3 7 1 0 8 4 5 5 1 5 9 4 5 3 5 1 3 9 4 5 1 5 9 8 9 3 7 5 1 b

0 1 1 5 4 1 1 5 9 1 8 1 5 4 7 5 4 5 1 5 5 1 3 9 6 1 5 0 1 4 c
a.g. a.g.

5 1 1 9 4 9 3 7 1 8 4 5 5 1 7 9 9 4 5 5 1 3 5 4 8 5 1 5 9 5 d

3 7 5 1 3 0 1 0 9 3 6 5 9 4 6 5 4 2 5 1 1 1 1 2 2 1 1 1 5 4 e
a.

5 7 1 3 1 7 4 5 6 3 4 2 9 9 2 3 6 7 7 1 1 0 9 4 0 5 1 5 7 4 f

3 6 0 1 9 4 5 1 8 1 5 4 5 1 8 8 4 5 3 4 9 5 1 1 9 5 6 4 5 1 g
a.c. a.c.

1 9 9 3 6 7 1 8 4 5 5 1 9 5 4 4 5 5 1 3 5 4 5 1 3 5 5 9 3 7 h

5 1 0 1 5 1 2 i

247 Elemente
247 elements

IA 5 b - 1

IA56

Doc ID: 6592461

Dinome substitution with systematic null
Zweistelliger Fallencasar mit systematischem Nenner (22 Br (Fk))

Plain elements / Klarelemente	a b c d d e f g h i j k l m n o p q r s t u v w x y z ⊙
Cipher elements / Codeelemente	26 09 68 56 18 45 91 01 63 15 46 06 77 27 57 88 43 92 42 11 99 37 84 30 85 53 35 12

Parallel passages
Parallelstellen

a 8: 0 9 3 6 5 9 4 3 5 4 2
e 8: 0 9 3 6 5 9 4 6 5 4 2

a 20: 1 1 5 6 2 4 5 1 1 5 2 3 7 1 0 8 4 5 5 1 9 9 4 5 3 5 1 3 9 4 5 1 5 5 8
g 23: 1 1 9 5 6 4 5 1 1 9 5 3 6 7 1 8 4 5 5 1 9 9 4 4 5 5 1 3 9 4 5 1 3 5 9
c 30: 4 5 1 1 9 4 9 3 7 1 8 4 5 5 1 7 9 5 4 5 5 1 3 9 4 8 5 1 5 9

a 1: 1 8 1 5 5 4 5
c 10: 1 8 1 5 4 4 5
g 8: 1 8 1 5 4 5

Doc ID: 6592461

6. Monome-dinome substitution - Wechselstelliger Zahlencäsar.

Based on the same principle as the null, namely the disguising of the phase, is the monome-dinome substitution where the (cipher) groups vary in length as the name indicates. The substitution shown in Appendix I A 6 has 1- and 2-places with the frequent elements e, i, n and r represented by the single digit values 0, 3, 5, and 8, while all the other elements are represented by 2-place groups. The 4-place displacement count given on sheet 2 of the Appendix reveals the the parallel passages of the enciphered text on sheet 1. As is to be expected with this system the parallel passages show no regularity either in respect to length or interval (see sheet 4 of the Appendix). Since the length of the parallel passages may be odd or even and lengths differing by only one element occur, we can deduce that the system has groups of differing length. Which cipher groups are monome and which are dinome is shown by a comparison of the parallel passages. Thus a comparison of the passage 9 6 3 0 7 4 with the other passage 9 6 3 7 4 reveals that 0 is a 1-place element.

Since in line b of the cipher text the passage

3 5 2 7 7 7 5 4 4 4 9 3 is separated from the parallel passage

9 7 7 1 0 9 6 3 9 6 only by a 5, we learn that 5 is a 1-place element.

If these two monomes in the cipher text are designated as 1-place, we learn from parallel passage 3 5 2 7 7 7 5 4 4 4 9 3 that 3 is also a 1-place cipher element and then from the passage 5 8 3 9 6 3 0 7 4 4 7 etc. that 8 is a 1-place element.

After the four cipher elements 0, 3, 5 and 8 have been marked off as monomes in the cipher text, we have left between them only passages of even length, a sign that we have now discovered all the 1-place cipher elements.

After we have determined the length of the cipher elements, all the elements and groups occurring are easily identified in the square on sheet 3. The group count on sheet 3 then gives a clear picture of a substitution alphabet so that the rest of the solution causes no difficulty. In respect to the relations between the length of the plain text and that of the cipher text the monome-dinome substitution occupies a middle position between monoalphabetic or digraphic substitution on the one

Doc ID: 6592461

hand and dinome substitution on the other. The ratio between the length of the plain text and the cipher text is 1 : 1 for the simple monoalphabetic substitution or the digraphic substitution and 1 : 2 for the dinome substitution but is approximately 1 : 1-1/2 for the monome-dinome substitution if the monomes are used for frequent elements.

Even though a study of the parallel passages permits us to recognize quickly that the groups differ in length and consequently the security of the monome-dinome substitution is not very great even when its use is closely restricted, we must not on that account underestimate the principle of using groups of varying length. Since the use of varying lengths signifies a constant interruption of the systematic character and since systematic structure lessens the security of any system, the principle as such is good. The use of this principle is all the more successful when a system yields few parallel passages because it is then more difficult to recognize the use of the principle than in our little example, provided it can be still recognized at all.

Doc ID: 6592461

TOP SECRET

1 2 3 [redacted] 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 [redacted] 5 6 7 8 9 0

Klartext: / Plain text

dernniederschlagsmangelvonsvebe	1
nzütrockenenmonatenwürdedürchd	2
enüeberschüssederrüebrigenmonate	3
aüsgeglichenobesondersniedersc	4
hlagsreichwürdedernovemberdess	5
ennniederschlagsmengedasdreifac	6
hedesnormalwertserreichte ⊙	7

Geheimtext / Cipher text

9 6 3 0 5 8 3 9 6 3 0 7 4 4 7 1 4 4 4 6 6 7 4 2 7 4 4 5 6 6	a
3 1 4 4 6 7 7 5 7 4 8 3 1 7 3 5 6 4 7 1 4 9 0 7 7 2 1 9 1 3	b
5 3 5 2 7 7 7 5 4 4 4 9 3 5 5 7 7 1 0 9 6 3 9 6 7 1 0 4 7 9	c
6 3 5 7 1 3 1 7 3 0 7 4 2 1 2 9 7 1 7 4 7 4 9 6 3 0 7 1 3 1	d
7 0 8 6 6 3 5 2 7 7 7 5 4 4 4 5 3 4 4 7 1 7 4 6 6 3 6 6 1 4	e
8 4 7 3 5 2 2 1 7 3 7 4 7 7 5 9 6 3 0 7 4 5 8 3 9 6 3 0 7 4	f
4 7 1 4 4 4 6 6 7 4 0 3 8 4 7 5 7 7 1 0 9 6 3 9 6 3 0 5 7 7	g
4 6 3 2 7 1 7 3 0 9 6 3 7 4 7 4 3 5 5 8 3 9 6 3 0 7 4 4 7 1	h
4 4 4 6 6 7 4 2 7 3 5 6 6 3 9 6 4 4 7 4 9 6 0 3 8 6 2 4 4 4	i
7 3 9 6 3 7 4 5 7 7 0 2 7 4 4 1 4 3 7 3 0 4 9 7 4 3 0 0 3 8	j
4 7 4 9 3 2 2	k

206 plain elements
206 Klarelemente
307 cipher elements
307 Geheimelemente

IA 6

TOP SECRET

Doc ID: 6592461

Wechselstelliger Zahlenschlüssel (1+2Zahl)

Monome-dinome substitution

Klarelemente Plain elements	a b c ch d e f g h i j k l m n o p q r s t u ü v w x y z ⊙ ⊙
Chiffrierelemente Cipher elements	44 17 21 47 56 36 26 62 98 42 21 14 27 57 72 49 12 0 77 93 11 46 37 41 19 64 22 67

Vierstellige Verschiebungsstatistik des Geheimtextes

4-place displacement count of the cipher text

00 38j.
1
2 77j.
3 44a.86i.84j.
4 79c.97j.
5 83a.77g
6
7 44a.72b 42d 13d 48f 44f 44d
8 66e.
9 63c.63g 63d.
10 66c 47c.96g.
1
2 97d
3 53b 13d 17d.
4 44a.46b.90b.84e.44g.44d 57j.
5
6
7 35b.30d 47d 08d 46a.37f 30d.
8
9 13b.
20
1 56b.29d 73f.
2 17f.
3
4 44i.
5
6
7 44a 77c 78e 17d.35i. 44j.
8
9 77d.
30 58a.77a.77d 77d 77f 77f 57g 96d
77d.43j'.03j.
1 46b.73b 73d 70d.
2 77d.
3
4 47e.
5 64b.35b.27c.97c.77d 27d.22f 58d.
66i.
6 61e.
7 47f 47d.45j.
8 47g.62i.47j.

39 63a.67c.63f 63g 63d.64j.63j.
40 38g
1 45j.
2 44a.12d 73i.
3 55d.00j.
4 77a 46a 66a 56a.67b. 49c 93c
49e.93e. 77a.77d 46g 44f
77d.46c.66d 44a.47j.73c.14j
5 66a.83f 47j.
6 67a.77b.63e.67g.32d.67i.
7 14a.14b.96a.48d.17e.35f.75f
14g.97g 43d 17d 49i.35i.43j
8 77b.47e.
9 03b.35c.63d 34e.60i.73j.44j.
32k
50
1
2 77c.77e.21f.
3 52c.
4 44c.44e.
5 83d.
6 63a.47b.63i.
7 48b.13d.44g.70j.
8 39a.33f.39d.
9 77c.63f.
60 38i.
1 48e.
2 44i.
3 05a.07a.14a.96c.57d.07d.52e.
66e.07f.03f 96g.05a 22d.44d 03d
36i.44j.
4 77b.47i.
5
6 44a.77a.35e.36e.14e.44g.44i.
39d.
7 42a.75b10c.40g42i.
8
9
70 86e.22j.

71 44a.49b.09c.04c.77d 44d 77d.
44e.44g 03g 73d 44d.
2 19b.
3 56b 09d 62f.44f 03d 56d.96j
04j.
4 47a.22a.45a.83b.21d 44d 96d
66e.44f.68f.42d 03g 63g 44d 33d
47d 28i.36i.57j 41j.30j.42k.
5 44b.44c.44e.56f.
6
7 57b.21b.75c.54c.10c 75e 54e 63f
10g 46g 02j.
8
9 63c.77g.
80
1
2
3 76a.17b.96f.56d.
4 73f.79g.44j.
5
6 63e.24i.
7
8
9
90 72b.
1 35b.
2
3 53c.44e.22k.
4
5
6 30a.30a.39c 77c.35c.30d.30f.30f
03g.30g 37d.30d.44d.03i.03j.
7 77c 17d.47g 30j.48j.
8
9

IA 6-2

82

Doc ID: 6592461

~~TOP SECRET~~

Gruppenstatistik des Geheimtextes:

Group count of the cipher text

		Häufigkeit / Frequency
0	a.a.b.c.c.d.d.e.f.f.g.g.g.h.h.i.j.j.j.	20
3	a.a.a.b.b.b.b.c.c.c.d.d.d.d.d.e.e.e.f.f.f.f.f.g.	41
	g.g.g.h.h.h.h.h.i.i.i.j.j.j.j.g.k.	
5	a.a.b.b.c.c.c.c.d.e.e.f.f.f.g.h.h.i.j.	19
8	a.b.e.f.f.g.h.i.j.	9
14	a.b.e.g.h.j.	6
17	b.d.d.f.h.	5
21	b.d.	2
22	f.k	2
27	a.c.e.h.i.j.	6
29	d.	1
44	a.a.c.e.e.g.i.i.i.j.	10
46	b.h.	2
47	a.c.f.g.g.h.i.k.	8
49	b.c.e.j.k.	5
62	i.	1
64	b.	1
66	a.a.e.e.e.g.i.i.	8
71	b.c.c.d.d.e.g.	8
74	a.a.b.d.d.d.k.f.f.f.g.h.h.h.i.i.j.j.	18
77	b.b.c.e.f.g.j.	7
91	b.	1
96	a.a.c.c.c.d.f.f.g.g.h.h.i.i.j.	15
97	c.g.j.	3

23 Elemente
23 elements

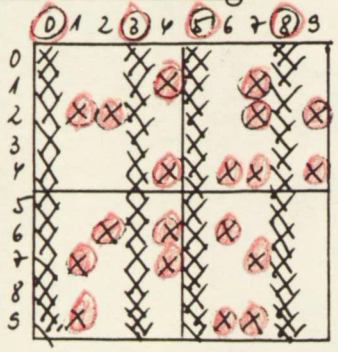
Anordnung der Geheimelemente nach der Häufigkeit.

Cipher elements in order of frequency

Geheimelemente / Cipher elements	3 0 5 7 4 9 6 4 4 8 4 7 6 6 7 1 7 7 1 4 2 7 1 7 4 9 9 7 2 1 2 2 4 6 2 5 6 2 6 4 9 1
Häufigkeit / Frequency	41 20 19 18 15 10 9 8 8 8 7 6 6 5 5 3 2 2 2 1 1 1 1
Klartext / Plain element	e r n s d a i h g ü o l m b t w c ö v h f z k

Gruppenbelegung

Groups occurring



I A 6 -3

~~TOP SECRET~~

Doc ID: 6592461

Parallel passages

Parallelstellen

Text	Stellung Position	Länge Length	Abstand Interval
96305	a1. g.24.	5 = 5	203 = 7·29
5839630744 7	a5. f22.	19 = 19	167 = 167
144466 74(27)	a19.	21 = 3·7	224 = 2·2·2·2·2·7
			57 = 3·19
963074	a8. f16.	6 = 2·3	158 = 2·79
3527755 44493	c2. e6.	12 = 2·2·3	64 = 2·2·2·2·2·2
97710963(96)	c15. g16.	8 = 2·2·2 10 = 2·5	121 = 11·11
71317	d4. d.27	5 = 5	23 = 23
47496	d20. i18.	5 = 5	148 = 2·2·37
03847	g11. j.28.	5 = 5	107 = 107
96374	i10. j3.	5 = 5	53 = 53

I A 6 - 4

Doc ID: 6592461

7. Polyalphabetic substitution with interrupted period (der Springcäsar)

With the possibilities already described a certain high water mark had been reached for the development of the 1-place monoalphabetic substitution and the dinome substitution. The further development of substitution systems could proceed in two directions.

Either the monoalphabetic method could be expanded to include two or more letters and the dinome expanded to three or more digits in order to further extend the method employed with some success in the syllable substitution or else several substitution alphabets rather than one could be used to encipher a text; that is to say one either went over to systems which made possible a greater number of variants and also the encipherment of greater amounts of traffic without endangering the security of the system or else by employing several substitution alphabets one reduced the amount of material enciphered by a single alphabet and at the same time reduced the number of parallel passages.

The former course leads from the substitution alphabet to the code. We shall discuss this possibility in connection with polyalphabetic substitutions because it has become the practice to differentiate the substitution alphabet, which works primarily with the individual element, from the code, which centers on the word, although basically there is no difference between substitution and code.

A change of alphabets when enciphering a text may take place only at certain intervals so that there are always several successive elements enciphered by one alphabet before one proceeds to the use of the second alphabet. This method has been given the name Springcäsar because in each case several columns are skipped before a change (of cipher alphabet) occurs. This change may be systematic, i.e. after a definite number of elements or columns, or it may be undertaken at varying intervals not fixed in advance. In the latter case it is necessary to indicate the use of a new alphabet by certain groups, so-called indicator groups, so that the decrypter may know when a change occurs and which alphabet has been used.

The significance of the indicator group is to give the decipherer certain

Doc ID: 6592461

clues to the system employed; in particular the indicator group shows which of several available systems is used and in what manner it is used. For this reason it becomes of great significance for the unauthorized decrypter if he can separate the indicator group from the rest of the cipher text and learn its meaning from its structure, its frequency, the time and position of its occurrence or other characteristics.

In Appendix 1 A 7 a the three cipher alphabets on sheet 2 were used to encipher the plain text on sheet 1, using alphabet I for columns 1 to 10, Alphabet II for columns 11 to 20, and alphabet III for columns 21 to 30. The parallel passages have been discovered by a one-place chain count (digraphic count). The resulting picture is not equalized, but shows no linguistic frequency curve. The parallel passages are interrupted. Their study reveals no regularity in respect to length or intervals. Since all the rather long parallel passages show interruption and the longest one shows two interruptions of like length, in each case with the same interval of 10, some regularities can be inferred. This is confirmed either by writing the cipher text out in a width of ten elements when all interruptions of th parallel passages occur either at the beginning or the end of this ten column block, or when the distances between the corresponding interruptions are counted.

1. From the beginning of the first interruption to the end of the second, i.e. including the interruption, and
2. From the end of the first interruption to the beginning of the second, i.e. excluding the interruption (sheet 3 of th appendix).

The study of these intervals then reveals in each case for one of the recovered interval values the factors 2 x 3 x 5 = 30 as common multiple. We reach the same result moreover either by adding together the intervals of a parallel passage and the length of their interruption or by subtracting them. The number 30 thus obtained along with the interval 10 found for several interruptions within one parallel passage shows the number of alphabets to be 3.

The most important characteristic of the systematic Springcäser is the fact

Doc ID: 6592461

that the intervals of the interrupting parallel passages give regular intervals if the number of interrupting elements is added or subtracted. The regular interval consists of the two factors: the change interval and the number of alphabets. The change interval is determined either by the interval of two interruptions within a parallel passage or by superimposing the cipher text with a columnar width such that the interruptions to the parallel passages form the beginning or end of the rows.

In Appendix I A 7 b, we have an example of the unsystematic Springcäsar. Four dinome substitution alphabets are employed to encipher the plain text; 1-place and 2-place indicator groups show the starting points (sheet 1, center). The alphabets are derived from one another by following a definite route and can therefore be reduced to one another as will be shown later (sheet 1, bottom).

The 4-place displacement count given on sheet 3 of the Appendix shows no linguistic frequencies in its totality. The parallel passages (see sheet 4) are predominantly even in length. The intervals are odd and even. It is striking that several rather short parallel passages follow one another in the same sequence and the interrupting passages either agree absolutely in length or differ but little from one another. Hence if the interrupting passages are subjected to close scrutiny, it appears that as a rule the one interruption begins with the number or with the group with which the corresponding interruption ends. If these repeated elements or groups at the beginning or end of the interruption are marked in the cipher text, then, if they are not counted, there remain:

1. Only even parallel passages,
2. Only odd intervals between parallel passages,
3. Even lengths of the passages interrupting the parallel passages.

If the 1 and 2-place groups thus marked in the cipher text are regarded as indicators announcing a change in alphabet, this explains the interruptions in the parallel passages. If the count of the cipher text is divided up according to the four indicator groups, we get a normal alphabet curve for each indicator (see sheet 5).

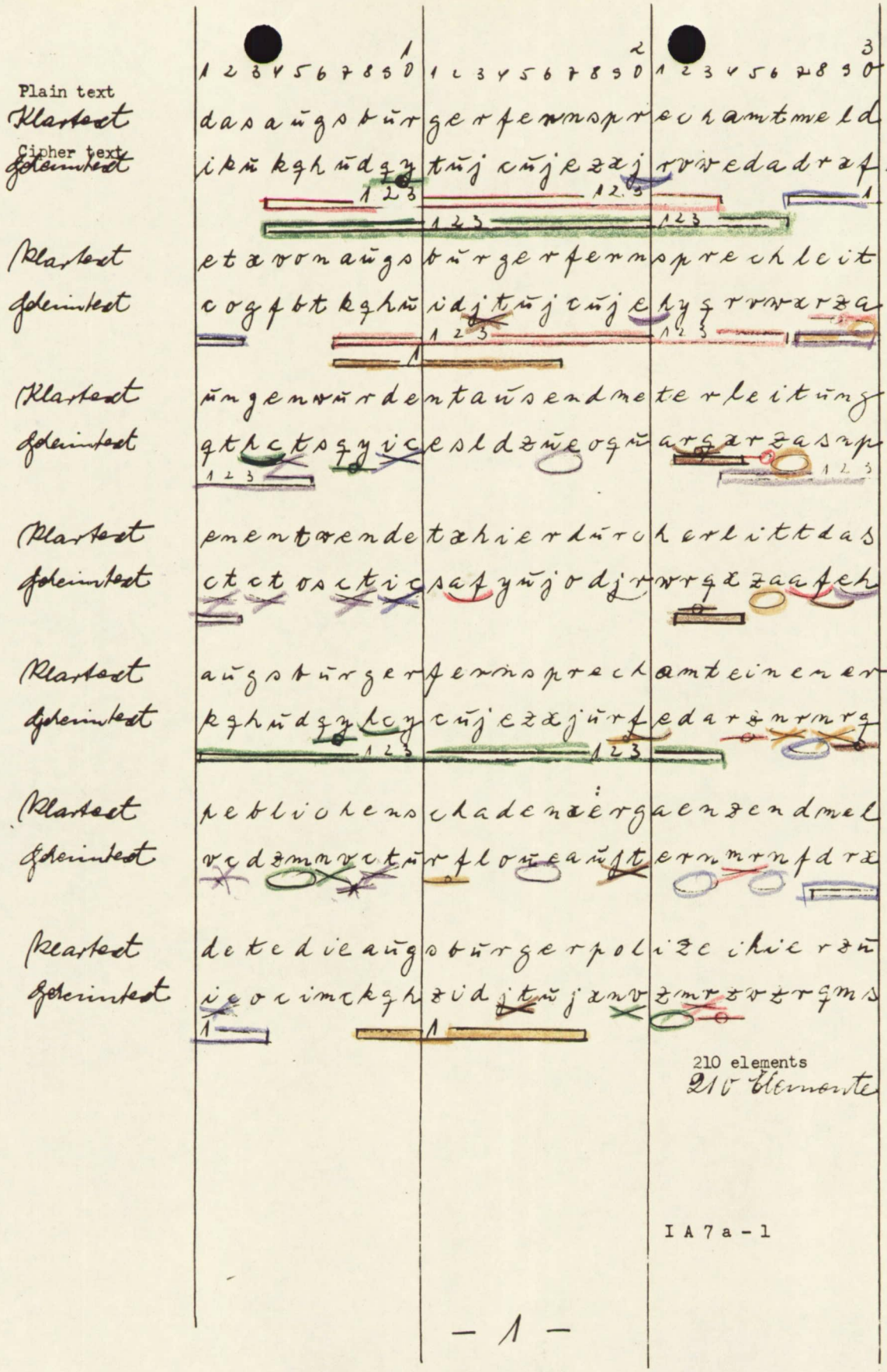
Doc ID: 6592461

As far as the security of the systematic or unsystematic Springcäsar is concerned, it is possible to multiply the amount of text permissible for the monoalphabetic substitution at least by the number of cipher alphabets used without having to fear any loss of security, provided the alphabets cannot be reduced to a common alphabet before solution.

Actually, however, the permissible amount of cipher material can be increased to a far greater degree than is indicated by multiplying the text length permissible for a single alphabet by the number of alphabets, the less the interval between changes is, if a certain minimum number of Springcäsars is employed simultaneously. If these conditions are met, the number of parallel passages is greatly reduced and the agreement between the plain-text picture and the cipher-text picture characteristic of monoalphabetic substitution is so broken up that it can no longer be recognized.

Doc ID: 6592461

IA7a



210 elements
210 Elemente

IA 7a - 1

Doc ID: 6592461

Drei Springcäsaren im Sprungabstand 10 (1 Buchst. 10 Buchst.)

3 substitution alphabets

Klarelemente / Plain elements	a b c d e f g h i j k l m n o p q r s t u ü v w x y z
Alphabet Cäsar 1	k d m i c r h v m p j z a t b w e y ü o q f s g x l
" 2	l i r o ü c t f y k h v q e n x b j z s d w m a p q
" 3	e k v f w t p w z c g x d n j y l q h a s o ü b i m

Einstellige Kettenstatistik

Digraphic count

des Geheimtextes.

a	d1 q3 r3 s3 f4 a4 l4 r5 ü6
b	t2
c	ü2 o2 ü2 t2 e3 t3 t4 t4 y4 y5 ü5 d6 t6 v6 i7 k7
d	q2 a2 r2 l2 z2 j4 q5 u5 z6 r6 q7
e	z2 d2 l2 s3 v3 k4 z5 d5 a6 r6
f	r2 t2 j4 e4 k5 l6 d6
g	f2
h	ü2 ü2 y2 c3 k5 ü5 c5 z7
i	k2 d2 c3 c4 l3 m3 d3
j	c2 l2 r2 t2 c2 e2 v4 r4 e5 ü5 t6 t7 x7
k	ü2 q4 q2 q5 q7
l	d3 v6
m	m6 r6 c7 r7 s7
n	p3 r5 r5 v6 m6 f6 v7
o	q2 q2 s4 d4 ü6 c7
p	c4
q	k2 y2 l2 r2 t3 y3 ü3 x3 z4 l5 y5 v6 l7 m7
r	v2 x2 v2 z2 q3 z3 v6 z4 f5 z5 k5 q5 f6 n6 w6 z7 z7 q7
s	q3 l3 k3 c4 a4
t	ü2 k2 a2 l3 s3 c4 o4 i4 ü4 k6 ü7
u	k2 d2 q2 q2 i2 q2 q2 p3 a3 j4 d5 j5 r5 r7 e7 j6 q7
v	v2 v2 c4 c6 z7
w	p2 z2 r4 z7
x	j2 f2 r2 t2 z4 j5 l7 m7
y	k4 q2 l3 u4 k5 c5
z	z2 a2 ü3 a3 a4 x5 m5 m7 l7 m7 v7 r7

Dreispalten-Walzenstatistik

3 column count

	I	II	III
a		II	IIII II
b	I		
c	IIII IIII III	III	
d	III	IIII	IIII
e		IIII I	IIII
f	I	III	III
g	I		
h	IIII I		II
i	IIII	II	
j		IIII IIII III	
k	IIII		
l		II	
m	II		III
n	I	I	IIII
o	III	III	
p			I
q	IIII III	I	IIII
r		III	IIII IIII IIII
s	II	II	II
t	IIII II	IIII	
u	IIII	IIII IIII II	
v	II	I	II
w			IIII
x		III	IIII
y	IIII	I	I
z	I	IIII	IIII II

I A 7 ▲ - 2

Doc ID: 6592461

Parallel passages
Parallelstellen – Untersuchung

Geheimtext Cipher text	Stellung Position	Länge Length	Abstand Interval
kghü . . . hüjcüje . . . rovv	1/4. 2/7.	20 = 2.2.5	33 = 3.11
kghüdgy . . . cüjeoxj . . . eda	1/4. 5/1.	23 = 23	117 = 3.3.13
drx . co	1/27. 6/28	6 = 2.3	151 = 151
kgh . idjtüj	2/7. 7/8	10 = 2.5	151 = 151
xrxa . . . ct	2/27. 3/24.	9 = 3.3	27 = 3.3.3
rgxe	3/22. 4/22.	3 = 3	30 = 2.3.5

Intervals between interruptions of parallel passages
Abstände der Parallelstellenunterbrechungen

Geheimtext ~~Cipher text~~	Stellung ~~Position~~	Interval Abstand including einschließlich der unterbrechenden Interrupting passages	excluding ausschließlich der unterbrechenden Stellen
kghü . . . hüjcüje . . . rovv	1/4. 2/7.	36 = 2.2.3.3	30 = 2.3.5
kghüdgy . . . cüjeoxj . . . eda	1/4. 5/1.	120 = 2.2.2.3.5	114 = 2.3.19
drx . co	1/27. 6/28.	152 = 2.2.2.19	150 = 2.3.5.5
kgh . idjtüj	2/7. 7/8.	152 = 2.2.2.19	150 = 2.3.5.5
xrxa . . . ct	2/27. 3/24.	30 = 2.3.5	24 = 2.2.2.3

I A 7 a – 3

Doc ID: 6592461

TOP SECRET

IA76

Klartext
Plain text

1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0	
d e r b a y e r i s c h e r ü n d f ü n k e r h e b t e i n e	1
ü m f r a g e ü b e r d e n e m p f a n g s e i n e r s e	2
n d ü n g e n o d e r b a y e r i o d e r ü n d f ü n k s o	3
e d t e r i s s e n o b d e r e m p f a n g s e i n e r s e	4
n d ü n g e n v o n s t a r k e n s t o e r ü n g e n t e e	5
i n t r a e d t i g t w i r d o g e r a d e d e r a t e n d	6
e m p f a n g l e i d e t ü n t e r s t a r k e n s t o e r	7
ü n g e n o	8

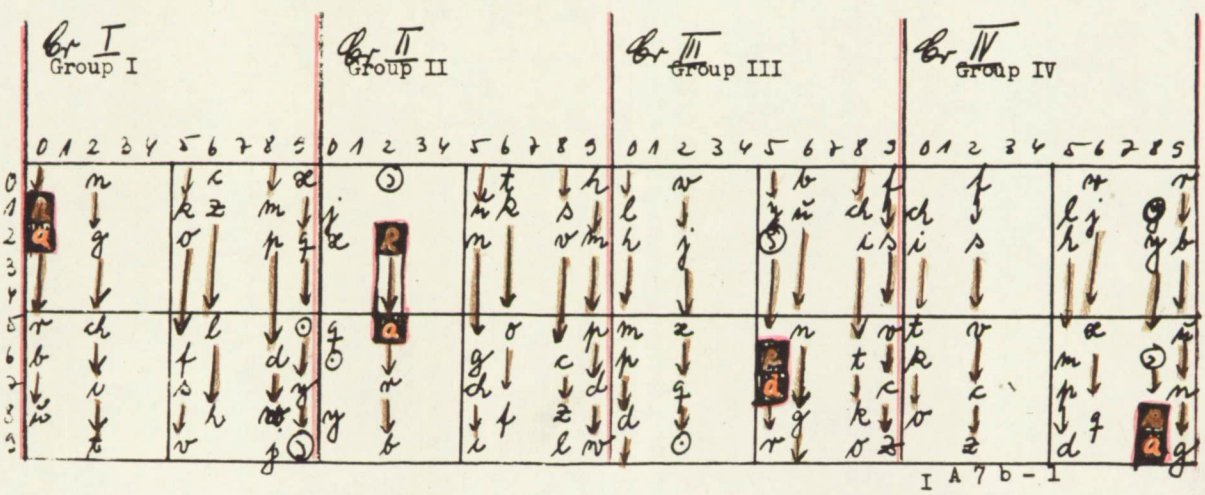
216 Elemente
216 elements

Vier Springcäsaren mit Kenngruppe (2 Ziffern)
4 alphabets with indicator groups (2 digit)

Klarelemente
Plain elements

Cäsar I	Kgr.	3	20 60 06 52 68 10 65 22 86 72 38 15 56 18 02 25 28 29 50 75 52 80 95 88 09 79 16 53 33
" II	"	4	52 92 68 75 79 22 86 65 09 35 10 16 98 29 25 56 53 50 72 18 06 15 28 35 20 80 48 60 02
" III	"	33	75 06 79 18 80 65 09 86 20 28 22 88 10 50 56 58 60 72 25 23 68 16 53 02 02 15 79 92 25
" IV	"	44	98 29 32 10 95 88 02 99 25 20 16 60 15 65 79 80 75 86 03 22 50 59 02 06 56 28 92 18 68

Ableitung obiger Cäsaren nach Durchlauf im Quadrat
Derivation of the above alphabets according to route in the square.

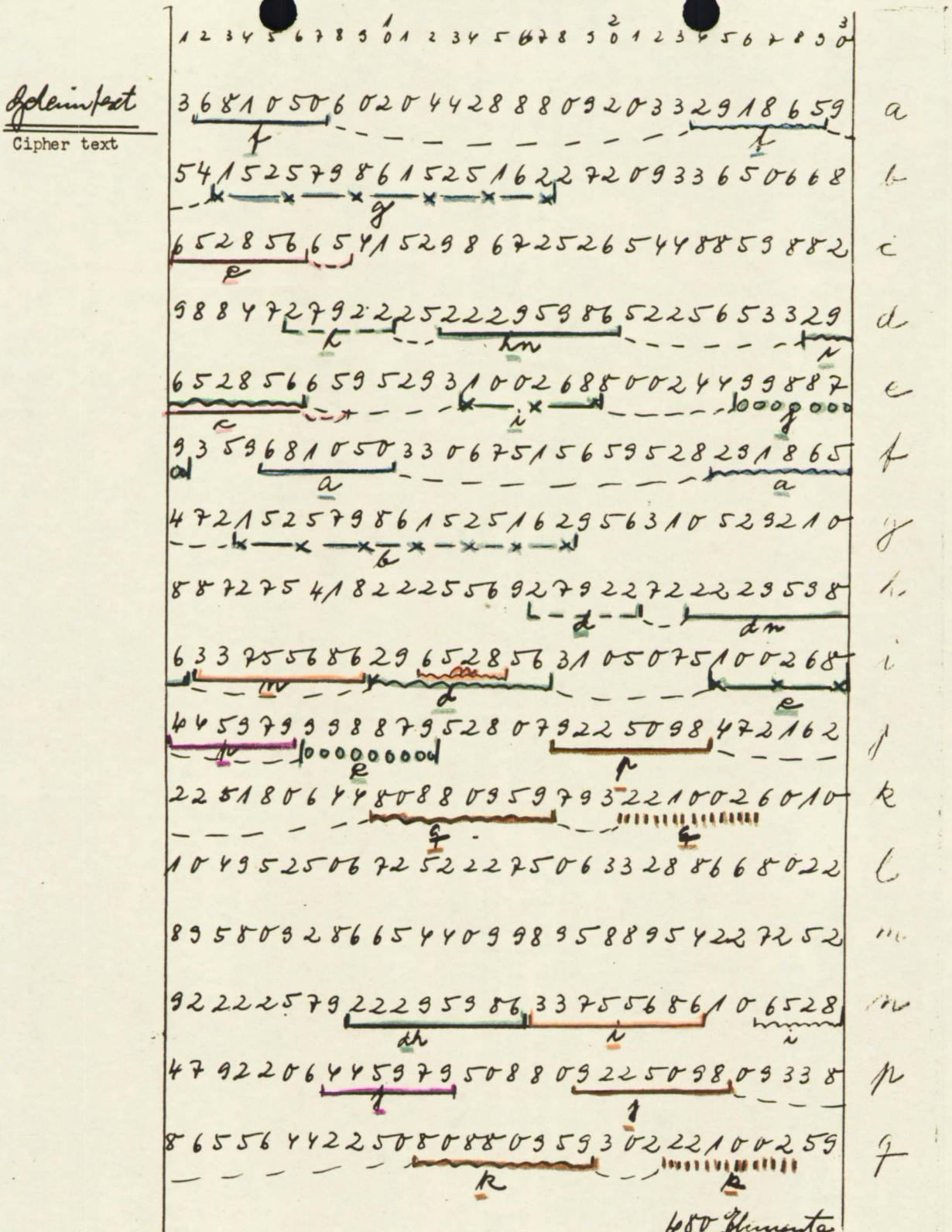


I A 7 b - 1

TOP SECRET

Doc ID: 6592461

~~TOP SECRET~~



– 2 –

~~TOP SECRET~~

Doc ID: 6592461

Vierstellige Verschiebestatistik des Schlüsselmittels

4-place displacement count.

00 26e 24e 26a 26k 25g
01 01k 04k
02 04e 68a 44e 68a 60k 28l 22g 53g
03 32a 30f
04 42a 95l
05 02a 03f 65f 26g 07i
06 02a 66k 75f 44k 32l 33l 52a 44p
07 51a 52j
08 83g 80k 80p 08q
09 20a 33b 87j 53k 28a 98a 22p 80p 33p 53g
10 57a 02e 57f 22g 88g 50a 02i 02k 10k 49l 02k65a
11
12
13
14
15 25l 25k 23e 25g 25g
16 22k 23g 02j
17
18 65f 22l 06k
19
20 44e 38a 93k 64p
21 52g 08g 62j 00k 09q
22 22k 25l 52d 29d 95d 57d 25l 55l 32l 32k 29l 95l 50j 25j 57k 10k 27l
23 75l 89l 02a 28a 95a 06p 50p 50q 24q 10g 22a 25a 57a
24
25 45a.
26 73k 14k 24c 32d 65l 83g 16g 56k 09j 18k 22l 23a 09p 72a 08q
27 97e 88e 89i 01k 06l.
28 40k 82d 54l 62l 22l 57l 25a
29 38a 56c 56e 25f 56i 04j 86l 95l 64a 47a
30 18a 86c 88c 53d 65d 34e 18f 56g 21g 59l 65i 22a 53a
31 67f 22q
32 09e 05g 05i
33 97e 36d 21k 88l
34 29a 65k 32d 06f 75a 28l 75a 88p
35
36 36e
37 81a 50b
38 55i 35a
39 86p
40 99a
41 52k 52c 52l
42 18a 89a 25q
43
44 28a 88c 95e 53j 80k 03a 58p 22g
45 57j 57p
46
47 30d 31g 21j 92p
48 85c 08k
49 91e 52l
50 60c 66b 33f 75i 58j 67l 63l 88p 58p 80q
51 62k 54f 62g 00i 80k
52 57b 51b 85c 58c 65c 32d 25d 85e 93e 02f 57g 51g 22g 85i 80j 57k 22l 89a 87a
53 32d
54 55b 85c 46c 72f 18k 40a 22a
55 65k 68i 68a 64q
56 65e 53d 65e 53f 31g 52k 86i 81i 80a 44q
57 98b 58g 22a
58 09a 83a
59 54c 18c 87d 32c 66e 52f 76k 79j 75k 18a 79p 30q
60 22a 40k
61 52b 52g 07a
62 39b 95g 96i 22j
63 10g 37i 10i 32l 37a
64 44k 45p 82q
65 95e 06b 28c 44c 44c 22d 33d 28e 95e 95f 47f 28i 44a 28a 54p
66 76b 51c 53a 60k 51a
67 45c. 51f. 25k
68 14a 65b 81b 10f 68i 44i 02l 04a
69 39k
70
71
72 09b 52c 79d 15g 98k 22k 16j 02l 52a
73
74
75 15f 64k 58i 10i 06l 58a
76
77
78
79 82b 22d 35e 82g 20k 99j 52j 22j 32k 32p 50p 28a
80 82a 02e 79j 64k 88k 25k 22l 52a 02p 93p 88q 55g
81 05a. 05f.
82 98c. 91f. 22k
83
84 72d 45i 22g 79a
85 66c 98c 66e 62i
86 15l 52b 32c 52d 51f 53a 05g 33k 29i 68l 65a 32a 40a 52p
87 23e 27k 55j
88 80a 05c 59e 23c 47d 08e 79e 72k 79j 05k 66k 51a 09p 65p 08q
89 58a 52a 57a
90
91 76e 84f
92 03a 22d 40g 72k 98k 35g 18a 28p 44p 32a 28a
93 36b 40e 53f 22k 38p 02q
94
95 40a 58d 29e 28f 63g 98k 28j 97k 25l 87a 82a 42a 58a 08p 93q
96 53c 52k 82e 52i
97 55j 52k 55p
98 61k 67c 82c 81d 65l 82e 64g 62k 83j 49j 95a 63a 05p
99 98e 98j 88j 83a

IA 7b - 3

Doc ID: 6592461

TOP SECRET

Comparison of parallel passages

Parallelstellen - Vergleich

Stellung, Position / Parallelstelle, Parallel passages

a 2
f 5

6 8 1 0 5 0 6 0 2 0 4 4 2 8 8 8 0 9 2 0 3 3 2 9 1 8 6 5 9 5 4 1 5 2 5 7 9 8 6 1 5 2 5 1 6 2
6 8 1 0 5 0 3 3 0 6 7 5 1 5 6 5 9 5 2 8 . . 2 9 1 8 6 5 4 7 2 1 5 2 5 7 9 8 6 1 5 2 5 1 6 2

d 6
h 17

2 7 9 2 2 2 5 2 2 2 9 5 9 8 6 5 2 2 5 6 5 3 3 2 9 6 5 2 8 5 6 6 5 9 5 2 9 3 1 0 0 2 6 8 8 0 0 2 4
2 7 9 2 2 7 2 2 2 2 2 9 5 9 8 6 3 3 7 5 5 6 8 6 2 9 6 5 2 8 5 6 3 1 0 5 0 7 5 1 0 0 2 6 8 4 9 5 9 7 9

Continued from / Fortsetzung von d 6 / h 17

9 9 8 8 7 9
5 9 8 8 7 9

j 18
f p 19

9 2 2 5 0 9 8 4 7 2 1 6 2 2 2 5 1 8 5 0 6 4 4 8 0 8 8 0 9 5 9 3 3 2 2 1 0 0 2
9 2 2 5 0 9 8 0 9 3 3 8 8 6 5 5 6 4 4 2 2 5 0 8 0 8 8 0 9 5 9 3 0 2 2 2 1 0 0 2

		Length / Länge	Interval / Abstände
a 2. f 5.	6 8 1 0 5 0 ——	6 = 2 · 3	153 = 3 · 3 · 17
a 24. f 25	2 9 1 8 6 5	6 = 2 · 3	151 = 151
b 3. f 4.	1 5 2 5 . . . . . 1 6 2	15 = 3 · 5	151 = 151
h 17. d 6.	2 7 9 2 2	5 = 5	131 = 131
d 16. h 24	2 2 2 5 9 5 8 6	8 = 2 · 2 · 2	131 = 131
d 29 i 10	2 9 6 5 2 8 5 6	8 = 2 · 2 · 2	131 = 131
j 18. f p 19.	9 2 2 5 0 9 8	7 = 7	151 = 151
f 10. f 12	8 0 8 8 0 9 5 9	8 = 2 · 2 · 2	152 = 2 · 2 · 2 · 19
j 1. f 8.	4 4 5 9 7 9	6 = 2 · 3	157 = 157

I A 7 b 4

75

TOP SECRET

Doc ID: 6592461

Vierspaltenstatistik des Geheimtextes

4 column count of the cipher text

Indicator group	3	4	33	44
02	𝍸 /		/	
06		////	//	
09		/		𝍸 /
10	𝍸 𝍸 /		/	
15		𝍸	/	
16		///		
18		//	//	
20	/			/
22	//	𝍸 𝍸 /		///
25		𝍸 𝍸 /		
28			𝍸 //	//
29		𝍸	𝍸	
50	///			𝍸
52	/	////		/
56		//	𝍸 /	
59	//	///		𝍸
60	//			
65		//	𝍸 𝍸 ///	
68	////		/	
72	/	𝍸 ///		
75	//	/	///	
79		𝍸 /		𝍸 /
80	/		//	///
86		𝍸 /	///	
88	/		/	𝍸 𝍸
92	/	//	/	
95		/	////	//
98				///
99				//

Groups occurring

Gruppenbelegung

	0	1	2	3	4	5	6	7	8	9
0			X				X			X
1	X					X	X		X	
2	X		X			X			X	X
3										
4										
5	X		X				X			X
6	X						X		X	
7			X				X			X
8	X							X	X	
9			X				X			X

Doc ID: 6592461

8. Periodic polyalphabetic substitutions - Die Spaltencäsaren.

Now if the change interval is further reduced, this leads ultimately to a change of alphabets from element to element or from column to column. In this case we speak of a Spaltencäsar (columnar Cäsar).

In Appendix I A 8 a three dinome substitution alphabets, derived one from the other, have been used in encipherment. The two place count made on sheet 2 of the Appendix in the number square shows only 29 different 2-place groups. This clearly reveals a 2-place character of the system so that a 2-place chain count is sufficient for a study of the cipher text.

The breaking up of the intervals between parallel passages shown on page 3 reveals a common multiple 2 x 3 = 6. Since a 2-place system is involved, this means that parallel passages can only occur at an interval of 3 columns. The complete analysis would then run:

1. The total count does not show linguistic frequency.
2. The frequency of parallel passages is less than in the plain text (theoretical frequency V_x with x cipher alphabets).
3. Length of the parallel passages is a multiple of 2.
4. Intervals between parallel passages are a multiple of 2 x 3.

A group count of the cipher text distributed over three columns (sheet 3), shows normal frequency for each column so that solution is similar to the solution of a simple monoalphabetic substitution. It is helpful to note the frequent cipher digraphs because this facilitates the transition from one column to the next.

The example given in the following appendix I A 8 b corresponds to the preceding in its method and analysis except that the five cipher alphabets were derived from one another by a different method to be explained later and that in so doing sixty different cipher groups arose which only appear in part in the count of the individual alphabets. The effect of the systematic character, due to the derivation of the alphabets from one another in both this and the preceding example, on the security of the system will have to be investigated separately later on.

Doc ID: 6592461

The further development of the Spaltenc&sar led to the so-called Tritheim table, named for the Abbot Tritheim who first recommended its use in the Middle Ages. The table shown in appendix I A 8 c sheet 1 consists of a square with 26 columns and 26 rows designated in each case by the coordinates a to z and contains the alphabet 26 times, displaced by one element in each line. The vertical coordinates correspond to the plain alphabet, the horizontal coordinates to the column designations, while the square itself contains the cipher elements.

The encipherment of a plain text is accomplished by first providing the elements of the plain text serially with the column designation from A to Z. Then each plain element can be enciphered with the associated cipher alphabet.

While in the table on sheet 1 both the single alphabets in the columns with their reversed alphabetic order and the horizontal rows are arranged quite systematically in the sequence of the alphabet, the tables can also be constructed so that:

1. As in the example given on sheet 2 of the appendix the individual alphabet in the columns has no systematic structure but all the follow-alphabets are derived from the first by the same rule so that the rows always show the same random alphabet with a different degree of displacement. The rows are termed transition rows because the sequence of letters contained in these rows shows how the cipher elements of one columnar alphabet change in passing from one column to the next.
2. As in the example on sheet 3 the alphabets in the several columns no longer show any outward kinship although they have been derived from one another by the same transition sequence as in the example on sheet 2. This table arose by transposing rows of the table on sheet 2.
3. As in the example on sheet 4 the columnar alphabets always show the same sequence of letters with a different degree of displacement but the adjacent alphabets can no longer be derived from one another by the aid of a transition sequence. This table on sheet 4 arose by transposing the columns on sheet 2.

4. As in the example on sheet 5 the columnar alphabets appear utterly random and do not allow any common transition sequence to be recognized. Nevertheless a systematic structure of the table can still be recognized inasmuch as each cipher element occurs once in each row and in each column. This table arose by a transposition of the columns of the table on sheet 3 which in turn was derived by transposing the rows of the table on sheet 2.

5. As in the example on sheet 6 each columnar alphabet is set up separately and independently of the others, so that an absolutely random table has resulted which is like the original Tritheim table only in outward form and in the number of alphabets but is otherwise a random polyalphabetic system.

Before taking up the question of the security of these tables, two other systems will be mentioned which belong here structurally, namely the so-called Communist system and the so-called book encipherment.

The so-called Communist system consists in enciphering very brief messages, often merely names or pass-words, by means of a key number by starting with the plain text letter and going ahead as many letters in the alphabet as is indicated by the appropriate digit of the key number. Thus if the key number reads:

1 2 3 4 5

and the plain text: h e u t e

then the cipher text reads: i f v u f

g w v g

x w h

x i

j

= i g x x j. In Appendix I A 8 d several short texts have been enciphered by this method. Now whether the encipherment is undertaken by counting ahead so and so many letters in the alphabet or whether the cipher letters are read off the table at the upper left on sheet 1, what is involved is nothing other than the Tritheim table with the limitation that instead of 26 columnar alphabets

only 10 are employed. The 10-column table shown on sheet 2 is constructed like the Tritheim table and can be used in the system under discussion.

Regarding the security of this method of encipherment we may say definitely that a single cipher text equal to the key number cannot be solved without knowing the key. It is a different story if the same key number is used a number of times and the unauthorized decipherer has several secret texts available. In this case it is well to write below each cipher text the possible plain text letters as has been done in Appendix I A 8 d. If now in the second sample text

the first possible plain letter is y,

the second " " " " x,

the ninth " " " " q,

then it may be assumed with a high degree of probability that the plain text does not begin with one of these letters. Correspondingly in the third sample text the 8th possible plain letter y can be ruled out as improbable. Since on the other hand the correct plain text letter in all the sample texts must stand on the same level, the 1st, 2nd, 8th and 9th letter can be ruled out in all the examples as unlikely so that only the 3rd to the 7th and the 10th letter remain open as possibilities. After all improbable letters have been crossed off in the second and third columns in the same fashion, we can proceed as follows:

According to sample text 1 from among the remaining possibilities of forming digraphs in the first two columns, namely:

kd kb ka kw kv ku jd jb ja jw jv ju

id ib ia iw iv iu hd hb ha hw hv hu

gd gb ga gw gv gu dd db da dw dv du

only the digraphs:

ka ku ja ju id ha hu ga gu da du

are plausible. Corresponding to these digraphs in the other sample texts we find:

yu yb yh yb uk th tb sh gb ph pb

di df ci cf bo al af zi sf yl vf

pa pu oa ou nd ma mu la lu ia ju

na nu ma mu nd ka ku ja ju ga gu.

If we cross out the improbable digraphs here we have left only the column

ha

th

al

ma

ka

with no elimination as the sole survivor. After solving the first two letters there is usually only one possibility left for the following columns so that the rest of the solution comes automatically, especially since with the third digraph we already begin to see word beginnings.

Also the so-called Book encipherment, shown by an example in I A 8 e, is nothing other than the Tritheim table used in a different way. In the table on sheet 1 of the above mentioned appendix which is valid for the book encipherment the letters A to Z have been provided with numerical values from 0 to 25 and/or 26 to 51.

After the text from the book agreed upon has been written out beneath or above the plain text to be enciphered, the letters of the book text and the plain text are converted into the numerical values of the table and added and the letter corresponding to this sum is entered as the cipher value as shown in the line of text on sheet 1 of the appendix.

To show that here too we are merely dealing with the Tritheim table, the cipher values of this example have been framed in red in the square on sheet 1 of the appendix where the book text indicates the columns and the plain text the row. The connection of the individual values framed in red through the remaining values of the alphabet yields the Tritheim table.

In contrast to the Communist system it cannot be claimed without further ado that with book encipherment a knowledge of a single cipher text does not permit the unauthorized decipherer to attempt decryption. To explain this fact three plain texts have been enciphered with the given book text on sheet 2 of the appendix. The three resulting cipher texts have been continued downward 25 times alphabetically on sheet 2 and laterally on sheet 3 so that from the cipher

value x, for instance, the possible plain text values y z a b c d etc. are developed one after the other.

As with the Communist system it is now necessary to try to pick out the columns which, when placed side by side, yield plain text. We must not lose sight of the fact that the cipher text row itself may contain plain text columns. Starting with the first column $\frac{x}{l}$ the other columns from 0 to 25 are associated to this first column one after the other and the digraphs which look likely are written down. If to these remaining digraphs there is associated the third column with all its possibilities, we either see the beginnings of plain text or it is clear that the first column of row 0 was not the correct initial column, in which case the same experiment is tried with the first column of the next row and of the following row. Then the experiment is tried starting with the first column of the 23rd row. The combination with the second column of all the rows appears as follows:

ur us ut uu uv uw ux uy uz ua ub uc ud ue

il im in io ip iq ir is it iu iv iw ix iy

ir is it iu iv iw ix iy iz ia ib ic id ie

uf ug uh ui uj uk ul um un uo up uq

iz ia io ic id ie if ig ih ii ij ik

if ig ih ii ij ik il im in io ip iq

After striking out unlikely digraphs the following columns remain:

ur us ul um un

il im if ig ih

ir is il im in

From the 3rd columns we can associate to these remaining digraphs

urt unt

ilr ihr

ird ind

When we consider the 4th column we find as the sole remaining possibility

unte ihrt inde

The continuation comes as a matter of course since from the moment when plain text can be recognized the rows supplement each other.

What has been shown here with a depth of 3 letters can prove successful with a depth of only two letters although this calls for a greater expenditure of effort.

But since the cipher text has been developed from plain text and book text, the book text also being plain text, it is natural to try using this plain text for solution. Since the book text has shown which of the 26 possible degrees of displacement of the plain text is to be selected as cipher text, the cipher text line itself can be designated as a, the next line 1 as z, the second line as y, the third as x etc., just as has been entered in red in the appendix. Since the book text value = plain text value = cipher value, we must also get cipher value − plain text value = book text value. Thus if from cipher value x = 23 or 49 from row 0 we are to get in row 1 a plain text value y = 24 or 50, the book text value according to the equation 49 (cipher x) − 24 (plain y) = 25 must have the value 25 and therefore corresponds to the book text value z.

Taking into account the book text values the initial column in row 23 would no longer read $\overset{u}{i}$ but $\overset{q}{u}$. Now all the other columns may be expanded by this fourth letter and our previously discovered plain text would now give us four columns as follows:

deru

unte

ihrt

inde

Introducing the line of book text with 3 cipher texts gives us 4 lines of plain text, with 2 cipher texts it gives us 3 lines of plain text and in case of a single cipher text it gives us 2 lines of plain text available for study as described above.

However, since solution is possible with 2 lines of plain text, a single cipher text can be solved. In practice the work is greatly simplified by the fact that the possible lines of plain text are no longer written out one beneath the other in an alphabetic sequence a, z, y, x etc., but the associated book-text values are arranged in the order of alphabetic frequency, because then the columns most often used will stand at the top and will be tried first in our experiment.

If the columnar substitutions thus far discussed are studied with respect to their security, the following defects are found in the several systems which have given the possibility of solution.

The two polyalphabetic substitutions in appendices I A 8 a and I A 8 b with 3 and 5 alphabets respectively could be solved fairly easily because the regular course of the alphabets could be recognized through evaluation of parallel passages so that all the cipher groups could be distributed to the appropriate columnar alphabets. After this distribution the single columnar alphabet could be solved in a familiar manner.

It is clear that in these two cases the possibility of solution was to be ascribed primarily to regularity in the use of columnar alphabet and only secondarily to the small number of such alphabets. If, for instance, the three alphabets in appendix I A 8 a had not always been used in the same sequence 1 2 3 but also in the sequences 1 3 2, 2 1 3, 2 3 1, 3 1 2 and 3 2 1 and these in turn had been used in irregular sequence, then in spite of the small number of columnar alphabets far more cipher material would be needed before one could even think of analyzing the system.

In the case of the Communist system in appendix I A 8 d the use of the columnar alphabets in an irregular sequence has already been realized through the use of the key number. The result was that the single cipher text could no longer be solved no matter how long it might be. If nevertheless two or three cipher texts in the same key led to solution of the system, that is doubtless to be ascribed to the alphabetic structure of the columnar alphabets because the course of solution taken was based on this alphabetic arrangement.

The book encipherment on its part combines the defect of the Communist system, namely the alphabetic structure of the columnar alphabets, with the defect of the polyalphabetic substitutions in Appendices 1 A 8 a and b, namely the use of columnar alphabets in a regular recurring sequence. Even though the sequence caused by the book text in the use of the columnar alphabets does not show the regularity of a constantly repeated limited digit sequence,

Doc ID: 6592461

nevertheless the partial regularity, which is brought about by the plain language in the sequence of the columnar alphabets, is sufficient to rob the book encipherment of the security requisite for the single use of the book text as cipher key.

With this we have already made two important basic discoveries regarding the use of all systems of columnar substitution:

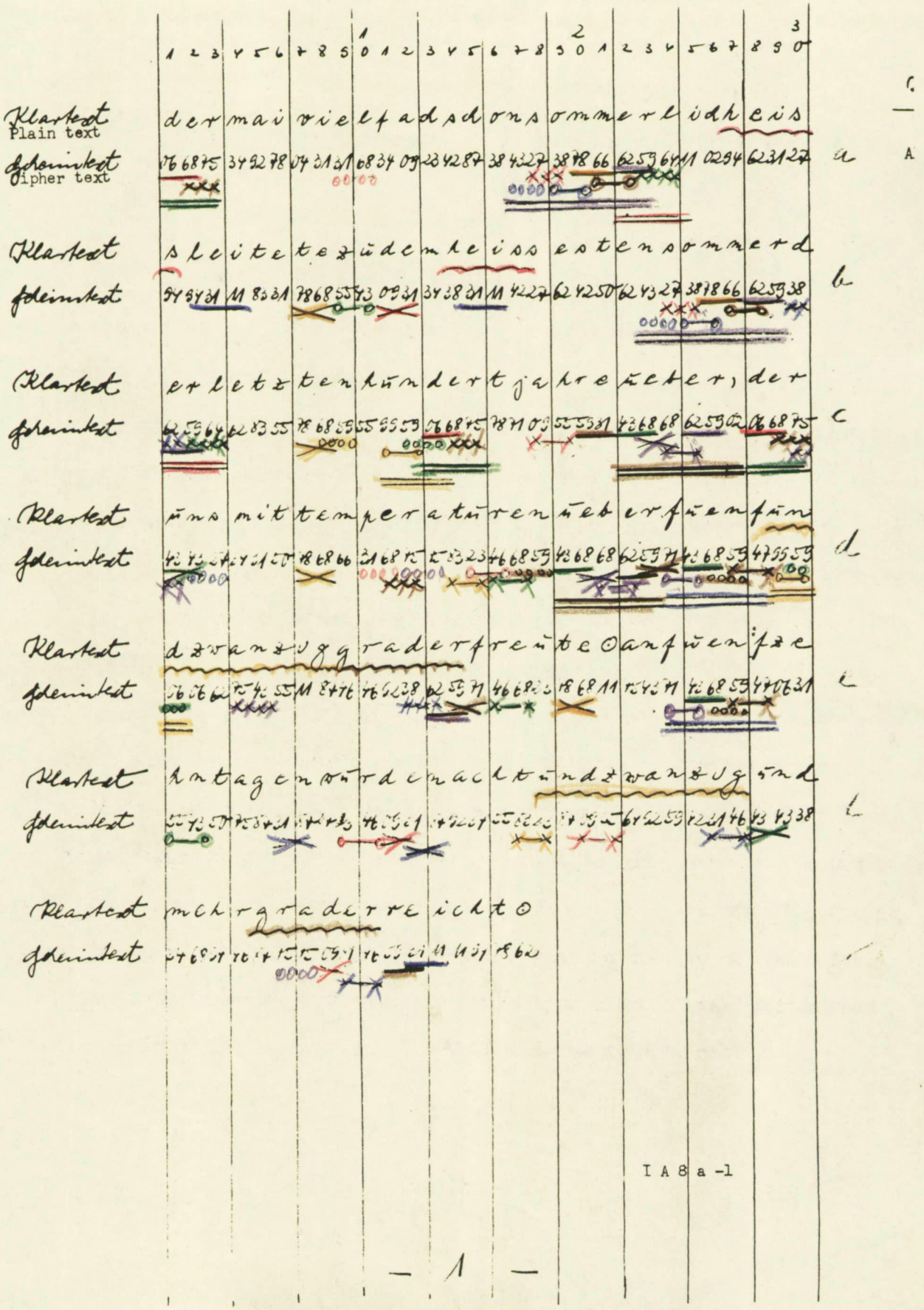
1. The columnar substitution must absolutely avoid any system in the succession of the columnar alphabets or must fix it so that from this system with a given amount of enciphered material no inferences can be drawn which might contribute to analysis and decryption.
2. The columnar alphabet must not have alphabetic structure. We must consider as equivalent to alphabetic structure any systematic structure which might be recognized, guessed, or the knowledge of which would lead to a solution of the cipher text.

The second requirement is not as essential as the first, so long as there is no possibility that two or more cipher texts in the same key can occur.

These two basic principles do not, however, cover all the dangers which may arise in connection with the use of columnar substitutions; because the security of a columnar system can be greatly impaired not merely by a systematic factor in the sequence of the columnar alphabets and in the structure of the individual alphabet, but also by any systematic relations or ties existing between one columnar alphabet and another. The following study will show this.

Doc ID: 6592461

~~TOP SECRET~~



IA8a

I A 8 a -1

— 1 —

~~TOP SECRET~~

Doc ID: 6592461

~~TOP SECRET~~

Substitution alphabets

dpaltoncasaren (dpa, Br)

Klarelemente / Plain elements	a b c d e f g h i j k l m n o p q r s t u v w x y z ⊙ ⊙
Chiffrier Alphabets I	75 27 50 23 06 62 47 92 55 11 02 09 68 34 87 38 31 71 46 94 78 43 04 64 66 53 42 83 99
" II	92 55 11 02 09 68 34 87 38 31 71 46 94 78 43 04 64 66 53 42 83 99 75 27 50 23 06 62 47
" III	09 68 34 87 38 31 71 46 94 78 43 04 64 66 53 42 83 99 75 27 50 23 06 62 47 92 55 11 02

Ermittlung der Gruppenbelegung

Determination of groups occurring

	0	1	2	3	4	5	6	7	8	9
0		×		×	×		×			×
1	×									
2			×					×		
3	×			×					×	
4		×	×				×	×		
5	×					×				×
6			×		×		×		×	
7		×					×		×	
8				×				×		
9			×		×					×

Zweistellige Kettenstatistik

Digraphic count

02	94a. 06c.
04	71a.
06	68a. 68c. 68e. 06e. 62e. 71e.
09	23a. 71b. 55c. 71f. 55f. 71g.
11	02a 83b. 42b. 87c. 75e. 11g 94g
23	42a. 46d 78e. 46f 87f.
27	38c. 94b. 62b. 38b. 34d 23f
31	71a. 68a. 27a. 11b. 78b. 34b. 11b. 43c. 50d. 68d. 55f 87f.
	87f. 46f. 46b. 11g.
34	32a. 09a 38b. 71d. 55f 68g
38	43a. 78a 71b. 78b. 62c. 62e. 34g
42	87a. 27b. 50c. 31f.
43	27a. 09b. 27b. 68c. 43d 27d 68d 68d 55e. 71e. 68a. 50f.
	43f. 38f.
46	68d 46e. 32e. 68e. 09f 43f 87g 53g
47	59d. 06e.
50	62b. 78d 75f.
55	43b. 78c. 99c. 59c. 11e. 43f. 83f. 64f.
59	64a. 38b. 64c. 55c. 06c. 31c. 02c. 43d. 71d. 47d 06e. 71e.
	47e. 42f. 31g.
62	59a. 71a. 42b. 43b. 55b. 59c. 83c. 59c. 59d 75e. 59e.
64	11a. 62c. 92f.
66	62a. 62b. 31d
68	75a. 37a. 55b. 59c. 75c. 68c. 62c. 75c. 66d 75d 59d 68d
	62d 59d 32e. 11e. 55e. 37g
71	09a. 43b. 46c. 43e.
75	37a. 78c. 43d. 75d 83d 43e 47f. 75g. 09g.
78	04a 66a 68b. 66b. 68c. 71c. 68d 68e 62g
83	71b. 55c. 23d 23f.
87	38a. 46e. 31f. 27f. 32f 09f. 75g.
92	78a. 38a. 37f. 55f.
94	62a 94b 31b. 46g 78g
99	53c 53d.

IA 8 a - 2

~~TOP SECRET~~

Doc ID: 6592461

Parallel passages
Parallelstellen

Text Text	Stellung Position	Länge Length	Abstand Interval
066875	a1. c13. c28.	6 = 2 · 3	72·2 = 2 · 2 · 2 · 2 · 3 · 3
			87·2 = 2 · 3 · 29
			15·2 = 2 · 3 · 5
432738786625 9	a17. b23.	14 = 2 · 7	36·2 = 2 · 2 · 2 · 3 · 3
625964	a22. c1.	6 = 2 · 3	39·2 = 2 · 3 · 13
995306	c11. d29.	6 = 2 · 3	48·2 = 2 · 2 · 2 · 2 · 2 · 3
4368686253	c22. d19.	10 = 2 · 5	27·2 = 2 · 3 · 3 · 3
7143685947	d24. e24.	10 = 2 · 5	30·2 = 2 · 2 · 3 · 5
Gesetzmässige Regularity		Länge = 2·x Length = 2 x X	Abstand = 6·x Interval = 6 x X

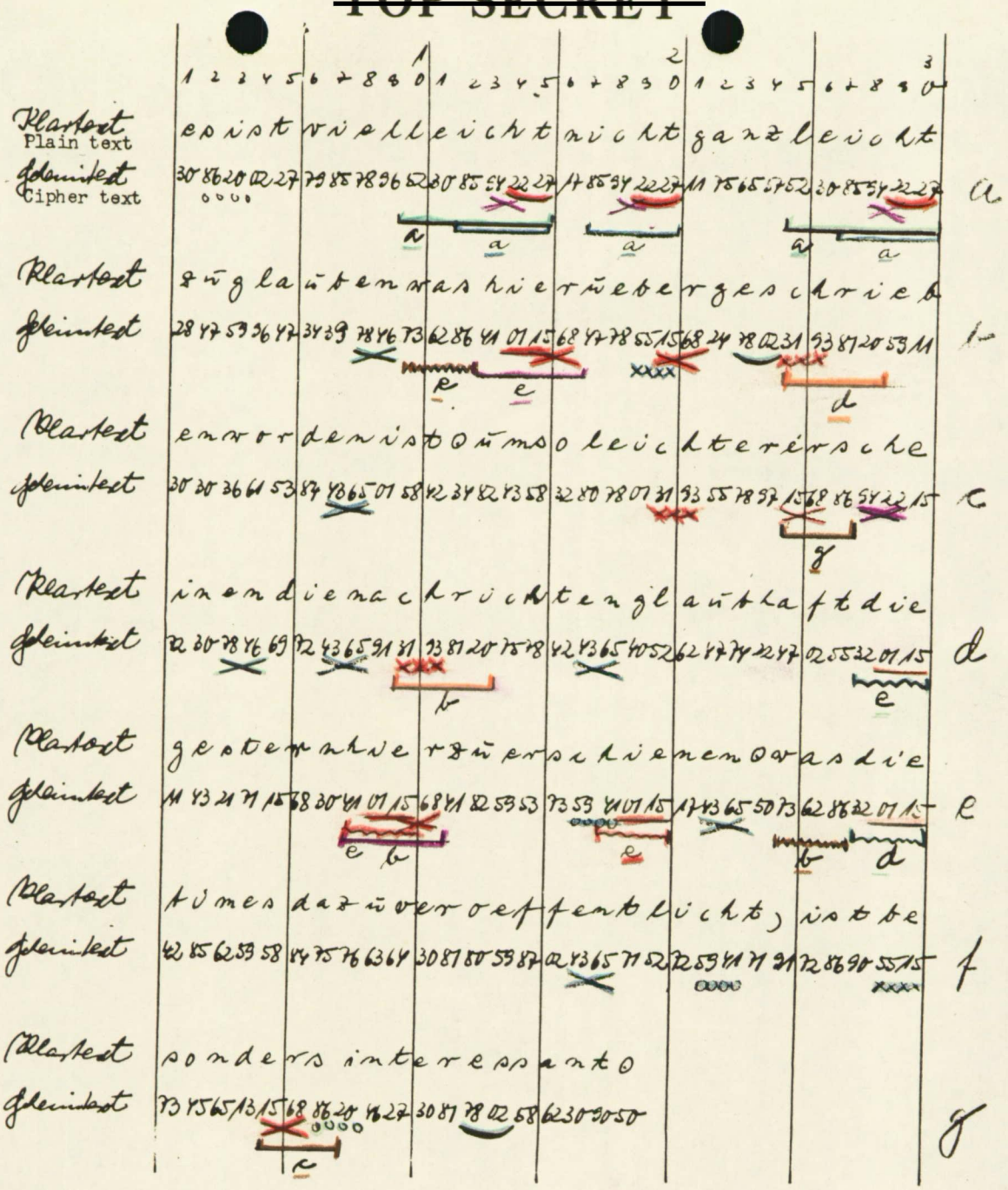
Spaltenstatistik der Gruppen
Columnar count of the cipher groups

	Gr I	Gr II	Gr III
02		I	I
04	I		
06	IIII	II	
09		IIII	II
11	𝍸	I	I
23	I		IIII
27		I	𝍸
31	I	IIII	𝍸 𝍸 I
34	IIII	I	I
38	III	I	III
42	I	III	
43	𝍸 II	𝍸 II	
46	𝍸 I		II
47	II		
50			III
55	IIII		IIII
59		𝍸 III	𝍸 II
62	𝍸 𝍸	I	I
64	I		II
66			III
71	I	𝍸 𝍸 𝍸	II
75		I	III
78	𝍸		𝍸
83	𝍸 I	II	I
87		IIII	
92	II	III	I
94	I	I	IIII
99		II	

IA 8a - 3

Doc ID: 6592461

TOP SECRET



IA8b-1

TOP SECRET

IA8b

Doc ID: 6592461

~~TOP SECRET~~

Alphabets
Spaltenväsaren (Spa 5 22 6r)

Spaltenväsar Alphabets	I	II	III	IV	V
a	62	75	10	91	47
b	26	29	74	55	11
c	46	59	94	75	31
d	84	27	22	13	69
e	20	42	48	53	15
f	02	15	50	21	87
g	11	24	39	40	96
h	53	06	71	22	78
i	12	85	20	07	52
j	37	50	85	66	22
k	54	67	02	83	35
l	67	80	15	56	52
m	14	27	62	43	99
n	17	30	65	46	02
o	32	45	80	61	12
p	47	60	95	76	32
q	63	76	11	92	48
r	68	87	16	97	53
s	73	86	21	02	58
t	42	55	90	71	27
u	24	47	82	63	19
v	75	82	27	08	64
w	88	01	36	14	72
x	94	10	45	24	82
y	50	63	58	75	25
z	28	41	76	29	12
ä	06	19	54	25	81
ö	21	34	69	50	06
Difference / Differens	+13	+35	+87	+56	

Determination of the cipher groups occurring.
Ermittlung der Gleichgruppen

	0	1	2	3	4	5	6	7	8	9
0		X	X							
1		X		X		X		X		
2	X	X	X		X			X	X	
3	X	X	X		X		X			X
4	X	X	X	X		X	X	X		
5	X		X	X			X		X	X
6		X	X	X	X	X			X	X
7		X	X	X	X	X	X			X
8	X	X	X		X	X	X	X		
9	X	X		X	X		X	X		

Parallel passages
Parallelstellen

Text	Stellung Position	Länge Length	Abstand Interval
52308594 2227	a 10. a 25	12 = [2] 2.3	30 = [2] 3 [5]
8594 2227	a. 12 a. 17.	8 = [2] 2. 2. 2	10 = [2] [5]
73 6286	b 10. e 15.	6 = [2] 3	190 = [2] [5] 19
4107 1568	b 13. e 8.	8 = [2] 2 2	170 = [2] [5] 17
31 9387 20	b 25. d 10.	8 = [2] 2 2	90 = [2] 3 3 [5]
15 6886	c 25. g 5.	6 = [2] 3	140 = [2] 2 [5] 7
3207 15	d 28. e 28.	6 = [2] 3	60 = [2] 2 3 [5]
4107 15	e 8. e 18.	6 = [2] 3	20 = [2] 2 [5]

—2—

I A 8 b – 2

~~TOP SECRET~~

Doc ID: 6592461

Zweistellige Ketten-Statistik
des Gydeintextes

Digraphic count

01	15b	31c	15e	15e					
	58c	15d	15e						
02	27a	55d	58g						
	31b	Y3f							
11	Y5a	Y3e							
	30c.								
13	15g								
15	68b	68c	68e	73g	12e				
	62b	72d	Y2f	68g					
17	Y5a								
	Y3e								
20	02a	75d							
	53b	Y6g							
21	71e								
22	27a	27a	Y7d						
	27a	15c							
24	78b.								
27	79a	11a	30g						
	17a.	28b							
28	Y7b								
30	Y6a	Y5a	36c	Y7f	50g				
	Y5a	30c	78d	87g	Y1e				
31	93b	93d							
	93c								
32	Y0c	01c							
	01d								
34	39b								
	42c								
36	61c								
39	78b								
40	52d								
41	01b	01a	01c						
	71f	82e							
43	34c	85f							
	Y3d								
45	65c.	65d	21e	65e					
	58c.	65d	65f						
47	65g								
48	73b	24g							
	63d								
47	55b	78b	02d						
	34b	74d							
50	73e								
	-g.								
52	30a	62d							
55	30a	72f							
56	84c								
	73e								
57	15b	32d							
	78c	15f							
57	12a								
58	Y2c	84f							
	32c	62g							
59	96b	11a	Y1f	Y1e					
	58f	87f	53e						
61	55c								
62	86b	53f	86e						
	Y7d	30g							
63	64f								
64	30f								
65	57a	51d	71f	50e					
	01c.	40d	13g						
68	Y1b	24b	98c	Y1e					
	86c	86g	30e						
69	72d								
71	52f	15e							
	21f								
72	30d	53f							
	Y3d	86f							
73	62b	59e							
	45g	62e							
74	22d								
75	65a	76f							
	78d.								
76	63f								
78	96a	55b	01c	Y2d					
	Y6b	02b	Y6d	62g					
79	85a								
80	78c								
	53f								
81	24b	87f							
	20d	78g							
82	Y2c								
	53e								
84	Y3c								
	75f								
85	78c	54a	62f						
	54a	57a							
86	20a	54c	20g						
	Y1b	50f	2e						
87	02f								
90	55f								
	50g								
91	31d								
	72f								
93	87b	87d							
	55c								
94	22a	22a							
	22c	22c							
96	52a								
	Y1b								
97	15c								

60 Elemente belegt
60 elements found

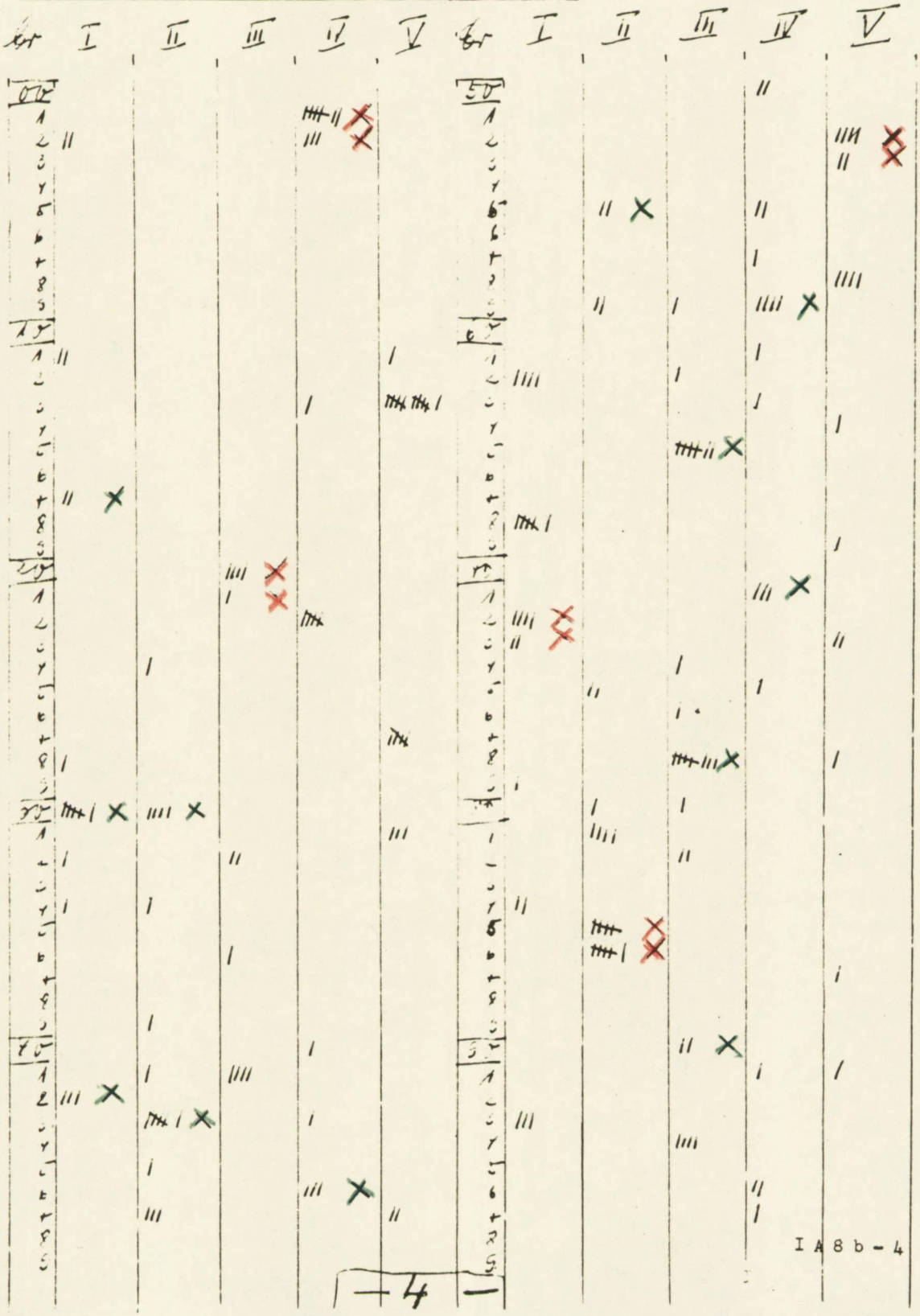
IA 8 b - 3

Doc ID: 6592461

~~TOP SECRET~~

Columnar count of the cipher groups.

Spaltenstatistik der Schlüsselgruppen



I A 8 b - 4

~~TOP SECRET~~

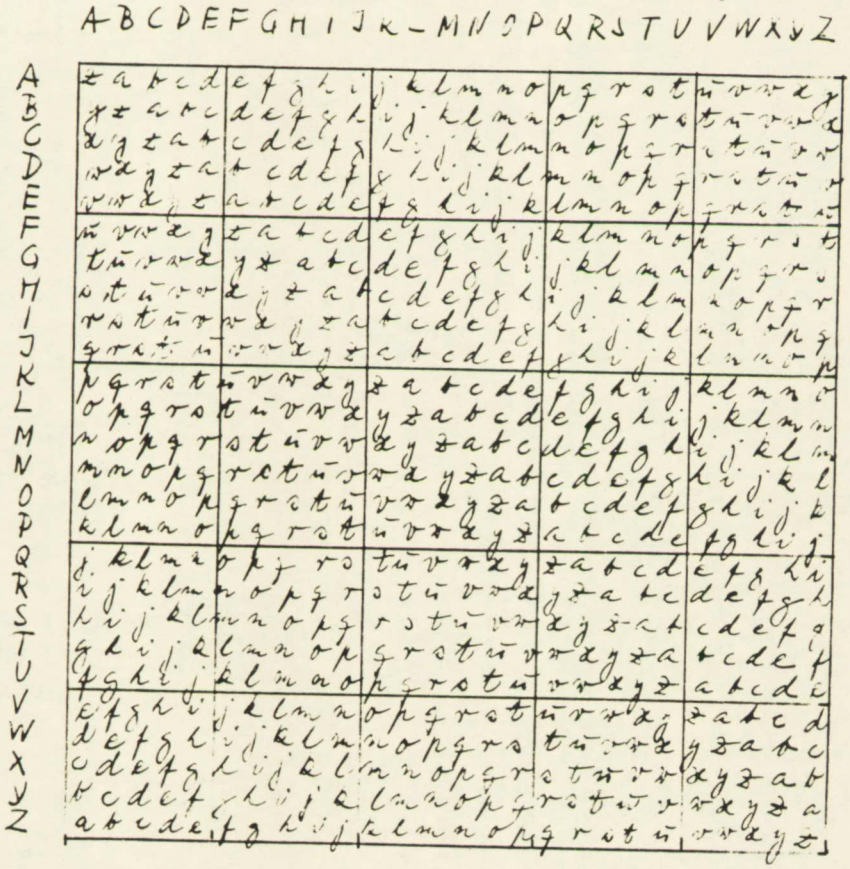
Doc ID: 6592461

Tritheimsche Tabelle

Tritheim Table

alphabetisch, reziprok, systematisch

normal alphabetic, reciprocal



Verschlüsselungsbeispiel:

Sample encipherment:

Klartext Plain text	erstbeispiel
Verschlüsselung mit Anfg. Encipherment starting with Column A	vjjjcamnadagyg
" Column B	wkkkdbovebcrzk
" Column C	xlllecpphcfsaw
" Column D	ymmmfdqiqgdgtbj

0 1 2 3 4 5 6 7 8 9 0 1 2 = 12/48/56/79

IA8c-1

IA8c

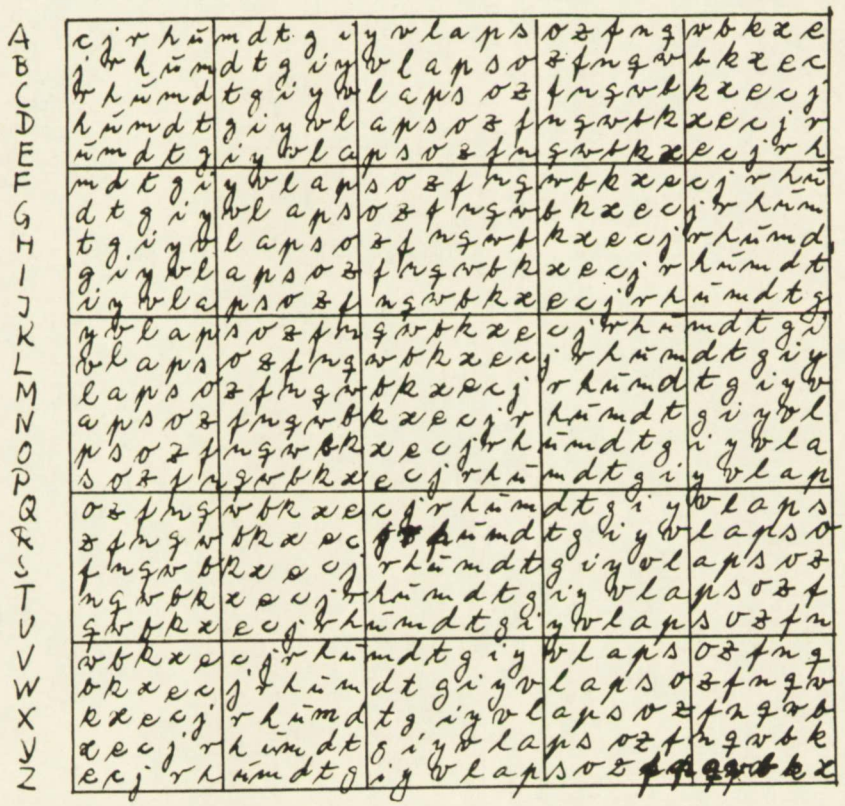
Doc ID: 6592461

~~TOP SECRET~~

Cäsar = Übergangsreihe

Alphabet = transition sequence

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z



Sample encipherment:
Verschlüsselungsbeispiel:

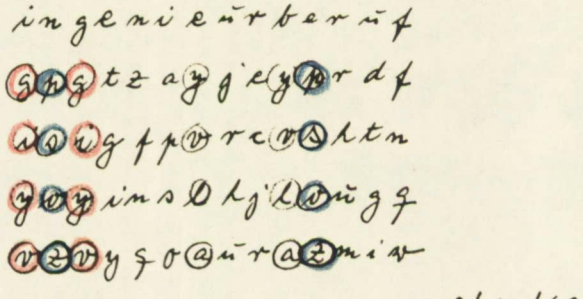
Plain text:
Klartext:

Starting with column
Verschlüsselung Spalte A ü. ff.

" " B "

" " C "

" " D "



0 1 2 3 4 5 6 7 8 9 0 = 2/10/63

0 1 2 3 4 5 6 7 8 9 0 = 9/58

I A 8 c-2

~~TOP SECRET~~

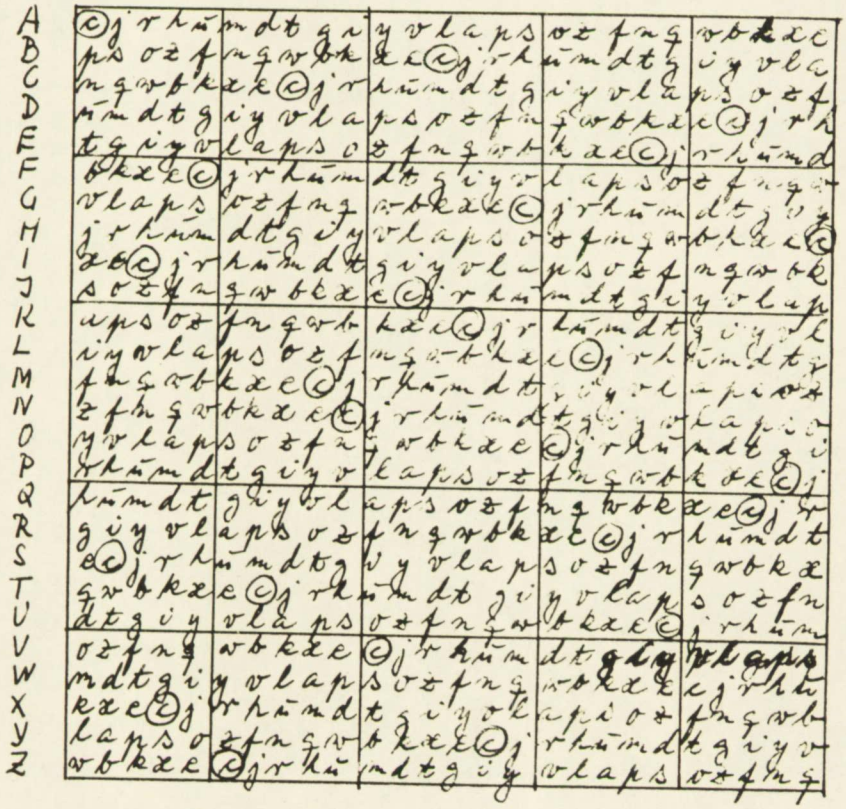
Doc ID: 6592461

~~TOP SECRET~~

abgeleitet von Seite 2
durch Zeilenvertauschung

Derived from page 2 by transposing rows

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z



Einsatzpunkt der
Starting point of the

Übergangsreihe
Transition sequence c j r h ü m d t g i y v l a p s ö z f n q w b k x e

in Spalte
in column A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

mit Klar
with plain a s i x f z t e n u v j b k y g o l r ä ü d q p h

Klartext
Plain text a s i e n s r e v o l t e

Starting with Column

abspalte A c c c y v u p h x n w m n

" B j j j w b m e x q q d s

" C r r r k d ö y u w t b

" D h h h a x t z z j b b g b

0 1 2 3 4 5 6 7 8 9 0 1 2 = 12/67/902

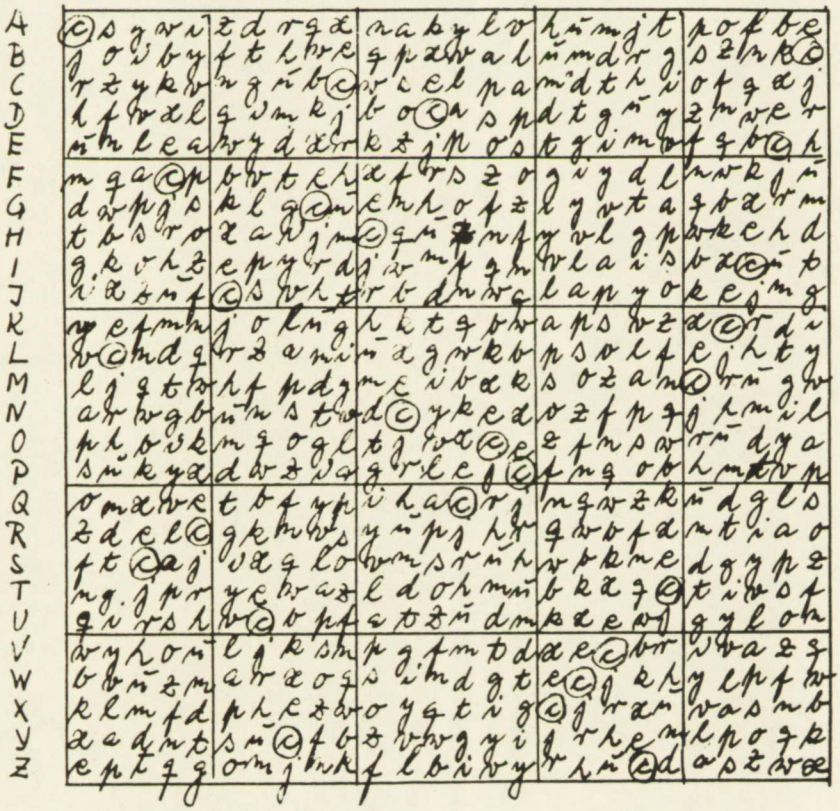
IA 8 c - 3

~~TOP SECRET~~

Doc ID: 6592461

abgeleitet von Seite 2
durch Spaltenvertauschung
Derived from Page 2 by transposing columns

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z



Einsabspringpunkte der
Starting point of the
Cäsaren alphabets cjrhümdtgiyvlapsozfngwbkxe

bei Klar with plain azyxwvütsrqponmlkjihgfedcb

in Spalte in column ATHQRSGUCENPOLVBWFXKIDYMJZ

Klartext plain text	ingenieurberuf	erstbestejger
Spaltencäsaren alphabets	ATHQRSGUCENPOL	AZJMYDIKXFWBV
Geheimtext cipher text	qnqtzaygeyrdf	üoookellbbebnm
Spaltencäsaren alphabets	THQRSGUCENPOLV	YDIKXFWBVLOPN
Geheimtext cipher text	ii ij ftpvrcvshtm 0 1 2 3 4 5 6 7 8 9 0 1 2 3	cllcnvqqfvfsj 0 1 2 3 4 5 6 7 8 9 0 1 2

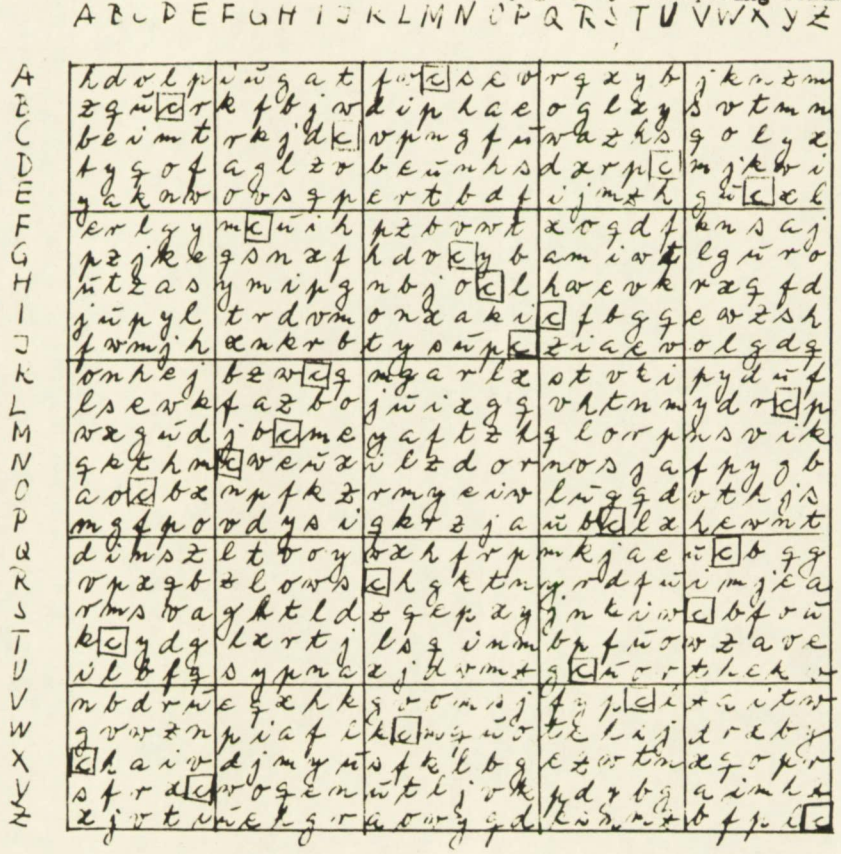
= 2/10/69/-

= 12/48/56/79

Doc ID: 6592461

abgeleitet von Seite 3
durch Spaltenvertauschung

Derived from page 3 by transposing columns



Transposition of columns:
Spaltenvertauschung:

M V Q A G Z B J H F T P D I E N C Y K X R L U W S O

Sample encipherment:
Verschlüsselungsbeispiel:

plain text
Klartext: a s i e n s r e v o l t e

alphabets.
Spaltencäsaren: M V Q A G Z B J H F T P D

cipher text
Geheimtext: c c c y v ü p p z n n n n

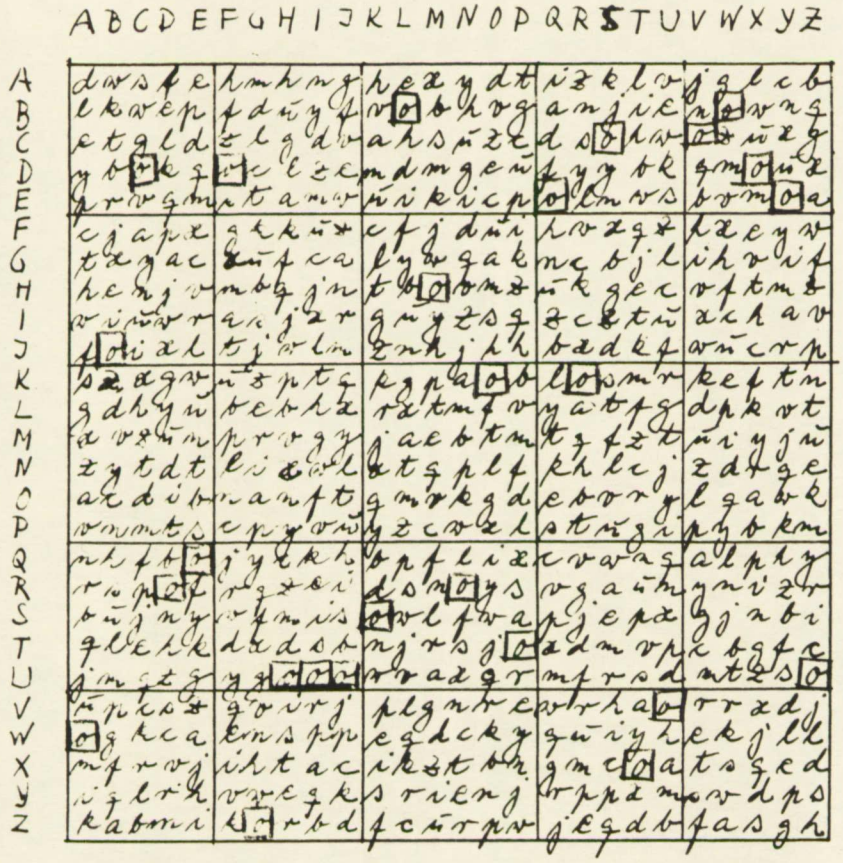
Spaltencäsaren: A G Z B J H F T P D I E N

Geheimtext: h h h a x t z z j b b g b

IA 8 c - 5

Doc ID: 6592461

unsystematisch
random alphabets



Verschlüsselungsbeispiel:
Sample enciphering:

Klartext
Plain text: c h o r a l

Verschlüsselt mit Spalte A usw.
Encipherment starting with Column A: E E d o k b

Column B: t n i f h c

C usw.: g j b r m b

IA 8c - 6

Doc ID: 6592461

TOP SECRET

ENCIPHERMENT TABLE FOR THE COMMUNIST SYSTEM

```
a b c d e f g h i j k l m n o p q r s t u v w x y z a b c d e . . .
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 . . .
  0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 . . .
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 . . .
      0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 . . .
        0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 . . .
          0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 . . .
            0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 . . .
              0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 . . .
                0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 . . .
                  0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 . . .
```

Key number: 6 4 3 1 0 7 4 1 7 1 5 8 6

1) Plain text h a r r i m e i e r

Cipher text n e u s s t i j l s

2) Plain text t h e o d o r f e l d e r

Cipher text z l h p n v v g l m i m x

3) Plain text a l b e r t s c h w a r z

Cipher text g p e f b a w d o x f z f

4) Plain text m a x h a m b u r g e r

Cipher text s e a i k t f v y h j z

5) Plain text k a r l g u t m a n n

Cipher text q e u m q b x n h o s

ENCIPHERING TABLE IN THE FORM OF A TRITHEIM

	1	2	3	4	5	6	7	8	9	1 0
A	b	c	d	e	f	g	h	i	j	k
B	c	d	e	f	g	h	i	j	k	l
C	d	e	f	g	h	i	j	k	l	m
D	e	f	g	h	i	j	k	l	m	n
E	f	g	h	i	j	k	l	m	n	o
F	g	h	i	j	k	l	m	n	o	p
G	h	i	j	k	l	m	n	o	p	q
H	i	j	k	l	m	n	o	p	q	r
I	j	k	l	m	n	o	p	q	r	s
J	k	l	m	n	o	p	q	r	s	t
K	l	m	n	o	p	q	r	s	t	u
L	m	n	o	p	q	r	s	t	u	v
M	n	o	p	q	r	s	t	u	v	w
N	o	p	q	r	s	t	u	v	w	x
O	p	q	r	s	t	u	v	w	x	y
P	q	r	s	t	u	v	w	x	y	z
Q	r	s	t	u	v	w	x	y	z	a
R	s	t	u	v	w	x	y	z	a	b
S	t	u	v	w	x	y	z	a	b	c
T	u	v	w	x	y	z	a	b	c	d
U	v	w	x	y	z	a	b	c	d	e
V	w	x	y	z	a	b	c	d	e	f
W	x	y	z	a	b	c	d	e	f	g
X	y	z	a	b	c	d	e	f	g	h
Y	z	a	b	c	d	e	f	g	h	i
Z	a	b	c	d	e	f	g	h	i	j

I A 8 d - 1

IA8d

TOP SECRET

Doc ID: 6592461

DECIPHERMENT

1

	n	e	u	s	s	t	i	j	l	s
1	[illegible]	d	[illegible]	r	r	s	h	i	k	r
2	[illegible]	[illegible]	[illegible]	[illegible]	q	r	g	h	j	q
3	k	b	r	p	p	q	f	g	i	p
4	j	a	[illegible]	o	o	p	e	f	h	o
5	i	[illegible]	[illegible]	n	n	o	d	e	g	n
6	h	[illegible]	[illegible]	m	m	n	c	d	f	m
7	g	[illegible]	[n]	[illegible]	l	m	b	c	e	l
8	[illegible]	w	[illegible]	k	k	l	a	b	d	k
9	[illegible]	v	[illegible]	j	j	k	z	a	c	j
0	d	u	[illegible]	[illegible]	i	j	y	z	b	i

2

	z	l	h	p	n	v	v	g	l	m	i	m	x
1	[illegible]	k	[illegible]	o	m	u	u	f	k	l	h	l	w
2	[illegible]	[illegible]	[illegible]	[illegible]	l	t	t	e	j	k	g	k	v
3	w	i	[e]	m	k	s	s	d	i	j	f	j	u
4	v	h	[illegible]	l	j	r	r	c	h	i	e	i	t
5	u	[illegible]	c	k	i	q	q	[illegible]	g	h	d	h	s
6	t	[illegible]	[illegible]	j	h	p	p	a	f	g	c	g	r
7	s	[illegible]	[a]	[illegible]	g	o	o	z	e	f	b	f	q
8	[illegible]	d	[illegible]	h	f	n	n	y	d	e	a	e	p
9	[illegible]	c	[illegible]	g	e	m	m	x	c	d	z	d	o
0	p	b	[illegible]	[illegible]	d	l	l	w	b	c	y	c	n

3

	g	p	e	f	b	a	w	d	o	x	f	z	f
1	[illegible]	o	[illegible]	e	a	z	v	c	n	w	e	y	e
2	[illegible]	[illegible]	[illegible]	[illegible]	z	y	u	b	m	v	d	x	d
3	d	m	[b]	c	y	x	t	a	l	u	c	w	c
4	c	l	[illegible]	[illegible]	x	w	s	z	k	t	b	v	b
5	b	[illegible]	[illegible]	a	w	v	r	y	j	s	a	u	a
6	a	[illegible]	[illegible]	z	v	u	q	x	i	r	z	t	z
7	z	[illegible]	[x]	[illegible]	u	t	p	w	h	q	y	s	y
8	[illegible]	h	[illegible]	x	t	s	o	v	g	p	x	r	x
9	[illegible]	g	[illegible]	w	s	r	n	u	f	o	w	q	w
0	w	f	[illegible]	[illegible]	r	q	m	t	e	n	v	p	v

4

	s	e	a	i	k	t	f	v	y	h	j	z
1	[illegible]	d	[illegible]	h	j	s	e	u	x	g	i	y
2	[illegible]	[illegible]	[illegible]	[illegible]	i	r	d	t	w	f	h	x
3	p	b	[x]	f	h	q	c	s	v	e	g	w
4	o	a	[illegible]	e	g	p	b	r	u	d	f	v
5	n	[illegible]	[illegible]	d	f	o	a	q	t	c	e	u
6	m	[illegible]	[illegible]	c	e	n	z	p	s	b	d	t
7	l	[illegible]	[t]	[illegible]	d	m	y	o	r	a	c	s
8	[illegible]	w	[illegible]	a	c	l	x	n	q	z	b	r
9	[illegible]	v	[illegible]	z	b	k	w	m	p	y	a	q
0	i	u	[illegible]	[illegible]	a	j	v	l	o	x	z	p

5

	q	e	u	m	q	b	x	m	h	o	s
1	[illegible]	d	[illegible]	l	p	a	w	m	g	n	r
2	[illegible]	[illegible]	[illegible]	[illegible]	o	z	v	l	f	m	q
3	n	b	r	j	n	y	u	k	e	l	p
4	m	a	[illegible]	i	m	x	t	j	d	k	o
5	l	[illegible]	[illegible]	h	l	w	s	i	c	j	n
6	k	[illegible]	[illegible]	g	k	v	r	h	b	i	m
7	j	[illegible]	n	[illegible]	j	u	q	g	a	h	l
8	[illegible]	w	[illegible]	e	i	t	p	f	z	g	k
9	[illegible]	v	[illegible]	d	h	s	o	e	y	f	j
0	g	u	[illegible]	[illegible]	g	r	n	d	x	e	i

JA 8d - 2

Doc ID: 6592461

~~TOP SECRET~~

Table: Tabelle:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51

Encipherment Verschlüsselung

Schlüsseltext Key book text	d	e	r	ü	n	t	e	r	g	a	n	g	d	i	e	s	e	s	c	h	i	f	f	e	s
Klartext Plain text	ü	n	t	e	r	d	e	m	e	i	n	f	l	ü	s	s	m	e	i	n	e	s	b	e	s	ü
Zahlenwerte Numerical equivalents	3	4	17	20	13	19	4	17	6	0	13	6	3	8	4	18	4	18	18	2	7	8	5	5	4	18
	20	13	19	4	17	3	4	12	4	8	13	5	11	20	18	18	12	4	8	13	4	18	1	4	18	20
Addition Addition	23	17	36	24	30	22	8	29	10	8	26	11	14	28	22	36	16	22	26	15	11	26	6	9	22	38
Geheimtext Cipher text	a	r	k	y	e	v	i	d	k	i	a	l	o	c	w	k	g	v	a	p	l	a	g	j	v	m

Tritheim table: Trithemische Tabelle

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
B	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a
C	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b
D	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c
E	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d
F	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e
G	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f
H	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g
I	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h
J	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i
K	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j
L	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k
M	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l
N	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m
O	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n
P	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
Q	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p
R	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q
S	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r
T	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s
U	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t
V	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u
W	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v
X	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w
Y	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x
Z	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y

IA8c

IA8e-1

— 1 —

~~TOP SECRET~~

Doc ID: 6592461

~~TOP SECRET~~

Key book
Buchtext — der ünterganges schiffes

Klartext / Plain text
1 — ünter des einflüsse eines besü
2 — chterlegram mes ostr ojenta
3 — in der verein igüng der vertrie

Chiffriert / Ciphered
Cipher text 1
1 — x r k y e w r i d k i a l o c v k q x a p l a g j o m
2 — l l i h r e i x z a z s y r q y i k l t p o j s x s
3 — k r ü y e o v i i k i a o j c r g d v j z l z y r m v

1 z — y p l z f x j e l j b / m m j o s f j y y b a / m s b z f p j g l j b

2 y — z t m a g y k f m k c / n n k p t g k z z c b / n t o a g g k k m k c

3 l — a ü n b h z l g n l d / o o l g ü h l a a d c / o ü x b h r l l n l d

4 m — b v o c i a m h o m e / p p w r v j m b b p d / p x y c i s m m o m e

5 v — c v p d j b n i p n f / q q n s v j n c c f k / q v z d j t n n p n f

6 ü — d x q e k c o j q o q / r r o t x k o d d q f / r x a e k ü o o q o g

7 t — e y r f l d p k r p h / s s p ü y l p e e k g / s y b f l k p p r p h

8 s — f z s g m e q l s q i / t t q v z m q f f i h / t z c g m v q q s q i

9 r — g a t h n f r m t r j / ü ü r v a n r q q j i / ü a d h n x r t t r j

10 q — h b ü i o g s n ü s k / v v s z b o s h h k j / v b e i o g s s ü i k

11 p — i c v j p h t o v t l / v v t y c p t i i i k / v c f j p z t t v t k

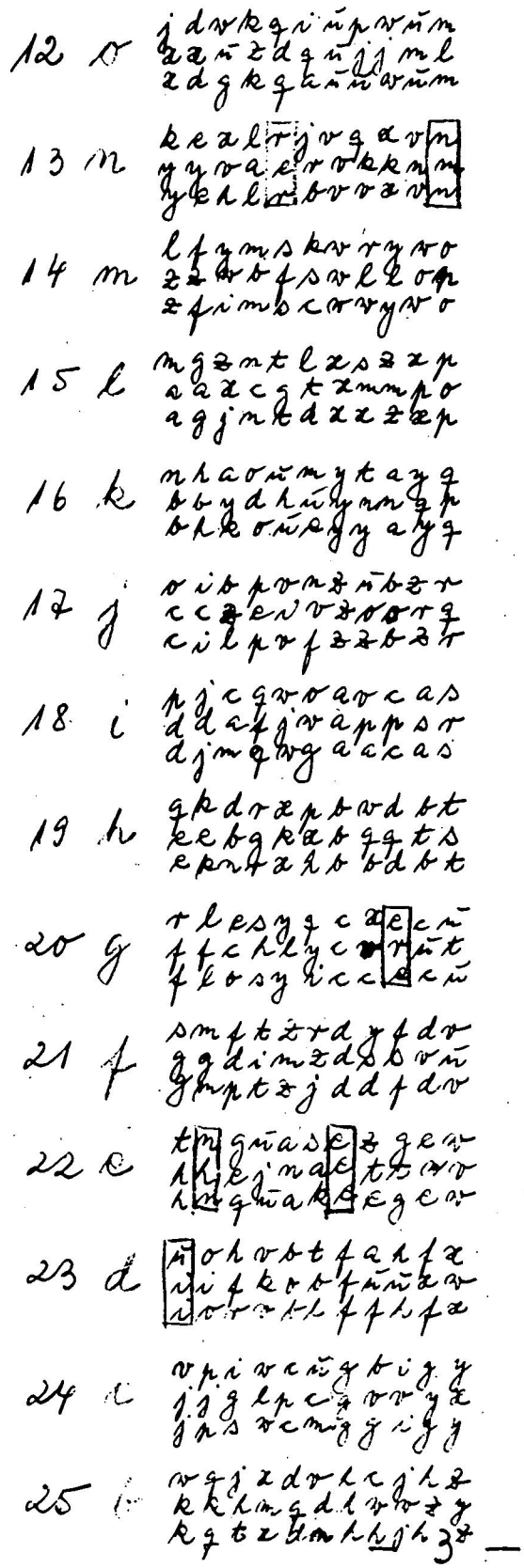
IA 8e-2

— 2 —

~~TOP SECRET~~

Doc ID: 6592461

~~TOP SECRET~~



IA8e-3

~~TOP SECRET~~

Doc ID: 6592461

9. Reduction of polyalphabetic substitutions.

As already mentioned in the discussion of the system employed in Appendix I A 8 a the 3 columnar alphabets used there were derived from one another. As a comparison of the three alphabets shown at the top of sheet 2 shows these contain the same sequence of cipher values displaced cyclically. We can conceive of this as if an alphabet from A to Z were inscribed on a strip of paper or a slide and moved along a second slide containing the numerical values underlying the above columnar alphabets. The above alphabets can then be read off at a given setting of the alphabet as plain sequence with respect to this numerical sequence as cipher sequence.

The same principle could also be applied to the Tritheim table shown in Appendix I A 8 c, since this table could also be read off from two strips or from a device like a slide rule where the one slide contains the plain sequence from A to Z of the coordinate column while the other slide bears the cipher sequence z to a, found within the square, inscribed twice so that all values can be read off in any position of the slide. The first columnar alphabet of the column A of the table would be set up on the slide when cipher z is set against plain A. The next alphabet B would be read off with cipher z set against plain B etc. Compared with the example previously given in Appendix I A 8 a the only difference is that the cipher sequence in the first case comprises numerical values and in the second case letter values.

The table shown on sheet 2 of Appendix I A 8 c can likewise be produced with such a slide where the plain sequence would be A to Z and the cipher sequence on the slide would be cjrhumdtgiyvlapsozfnqwbkxe. The setting of the slide would then be cipher c against plain A for columnar alphabet A, cipher j against plain A for columnar alphabet B, cipher r against plain A for columnar alphabet C, etc. It is then possible to enter the column designations A B C etc. beside the cipher values c j r etc., or to alter

Doc ID: 6592461

the column designations correspondingly.

Regarding all alphabets which can be derived in this fashion it may be said that they depend on the slide principle because one alphabet in relation to the next merely depends on a new setting of the plain sequence to the cipher sequence on the slide rule. In contrast to a system to be explained later we speak here of the short slide, because the slide contains only as many cells as the alphabet has cipher values associated to plain values.

In Appendix I A 9 a sheet 1 the three alphabets for Appendix I A 8 a have been listed as they were found by solving the sample text. Consequently the alphabets show gaps in the cipher sequences wherever certain plain elements of a column did not appear.

If these alphabets are based on a different setting of the cipher sequence in respect to the plain sequence on a slide it can be inferred that the cipher values of two alphabets on the slide which are associated to one plain value have the same interval as do all other pairs of cipher values of these two alphabets which are associated to one definite plain value.

Thus if it is assumed that the two cipher values 62 and 68 from alphabet I and alphabet II, which both correspond to the plain value e, have an interval x between, it follows that the cipher values 68 and 94, which are both equal to plain l, stand at the same interval x from one another, as do the pairs of cipher values 94 and 42, 42 and 06, 06 and 09, which correspond to the plain letters s, z and d respectively in alphabets I and II. In this way fragments of the transition sequence between two alphabets can be established which contain only cipher values with the same interval on the slide. The fragment for the values just given reads 62 - 68 - 94 - 42 - 06 - 09. At this point the transition sequence cannot be extended because the value 09 in alphabet I is missing due to the gaps.

On sheet 1 of the Appendix all fragments of the transition sequences between alphabets I and II, II and III, and I and III are listed and provided with the row designations 1 a - h, 2 a - g, 3 a - h.

A comparison of row 3 e with row 2 b shows that both sequences contain the cipher values 42 and 27. But since sequence 3 e contains two other values between these two we must assume an interval between the values of sequence 2 b which is divisible by 3 if we desire to unite the two sequences 2 b and 3 e.

On the other hand sequence 2 b and sequence 1 a agree in two cipher values, namely 42 and 62, while in sequence 1 a the values 62 and 42 are separated by two additional cipher values and in sequence 2 b the values 42 and 62 in the reverse direction are separated by one cipher value; a combination of these two sequences to form one sequence would presuppose that the direction of all sequences formed between alphabet I and alphabet II is reversed and that the interval between 42 and 62 is divisible by 6, so as to take into account both the interval divisible by 2 in sequence 2 b and the interval divisible by 3 of sequence 1 a. The combination of these two sequences 2 b and 1 a into a single sequence has been carried out on sheet 2 of the Appendix. Into the resulting transition sequence can be introduced readily the remaining fragments of sequences 1 b, 1 c, 1 d, 1 f and 1g. If later on the fragment from sequence 2 a is to be introduced, we get from the interval 92 . . 09 the total length of the slide as 29, since the interval from 09 to 92 is already fixed. If the fragments from the sequences 2 c, d, e, f and g are then to be introduced, we get almost the complete cipher sequence from which only one cipher value is missing, although the transition sequences between alphabet I and alphabet III have not yet been taken into account at all.

If, finally, the corresponding plain sequences for the three alphabets are produced, these sequences supplement one another until only four plain values are missing because they did not appear in the text of Appendix I A 8 a. Moreover in so doing we get through v = 04 the value missing in the cipher sequence as 04.

The appropriate slide settings for the plain and cipher sequences thus formed allow us to produce the alphabets I, II and III.

Doc ID: 6592461

A comparison of this slide with the original arrangement of the plain sequence and cipher sequence shown on sheet 2 reveals that, due to the first arbitrary assumption of a definite interval, the values which are adjacent on the original slide appear on the reconstructed slide at an interval of 21 from left to right or of 8 from right to left. In spite of the different structure, the two slides have the same effect. The reconstructed slide is therefore termed an equivalent or substitute slide.

Since the values which are adjacent on the original slide with its 29 cells can appear on the substitute slides at the intervals from 1 to 28, it is possible to produce 28 different slides, each differing from the other but having the same effect, of which one will coincide with the original.

The example on sheet 3 of the Appendix shows that with an original slide of 28 cells and the derived substitute slide it is possible that with certain intervals several fragments of substitute slides will be obtained instead of an entire substitute slide. From the comparison on sheet 4 of the Appendix showing:

1. Length of slide,
2. Interval on the substitute slide between adjacent values on the original slide, and
3. Data regarding the parts of which the substitute slide is composed, it is apparent that the least common factors of the length of the original slide and the intervals between the values on the original slide which are adjacent on the substitute slide indicate the division of the substitute slide. Inversely from the number of parts of the substitute slide and the total length of the slide an inference can be drawn as to the interval between the values on the original slide.

The 5 columnar alphabets derived from one another and shown in Appendix I A 8 b are based on the slide principle with this difference that the slide has for the 28 plain and cipher values not 28 cells but 100 cells designated on the cipher side from 00 to 99, in other words a long slide. The plain values are likewise on a slide with 100 cells distributed at optional

intervals and in any desired sequence. By setting plain a against cipher 62 we get alphabet I, with plain a against cipher 75 we get alphabet II and with plain a against cipher 10 alphabet III etc. Contrasted with the short number slide the difference in a purely external respect consists in the fact that with a short slide the cipher text shows only 25 to 30 different cipher groups because with the short slide the number of plain elements and cipher groups coincides, whereas with the long slide the number of resulting cipher groups increases with each new columnar alphabet. For instance, we get 60 different cipher groups from the five alphabets in Appendix I A 8 b.

A closer study of the long slide shows that - when the presence of the long slide can be surmised - the column count resulting after the evaluation of the parallel passages may profitably be entered at once in columns of 100 cells. If these columns with the frequency entries are slid with respect to one another so that the entries correspond as closely as possible in all columns with regard to frequency of occurrence, then we get the figure shown in Appendix I A 9 b where it has been possible to arrange that:

1. Frequent values generally stand on the same level with frequent values,
2. Infrequent values generally stand on the same level with infrequent values or with empty cells,
3. Occupied cells in a column correspond as far as possible in position with occupied cells in the other column.

Columnar alphabets derived with the long slide can therefore readily be reduced to one another before the individual alphabets can be solved. Inasmuch as this reduction can be undertaken with great certainty even though there are few entries in all columns, columnar alphabets derived from one another with the long slide hardly afford any greater security than the simple monoalphabetic substitution, no matter how great the number of columnar alphabets may be, unless it happens that the entries for the individual alphabets do not permit this simple reduction. The possibility of reduction <u>before</u> solution is based on the fact that the cipher elements are arranged in an arithmetic sequence, that is to say

in a sequence which is known before solution of the columnar alphabet.

If, on the other hand, the structure of the cipher sequences is neither arithmetic or alphabetic, as is generally the case when derived with a short slide, then a reduction of the columnar alphabets to one another is possible only after solution, since the arrangement of the cipher elements, in which a reduction is possible, can only be found when their plain equivalents are known. Hence the short slide with a random arrangement of the cipher sequences affords increased security. Of course one must not forget that even a partial solution of the columnar alphabets may afford possibilities of reduction. The greater the number of columnar alphabets, the less may be the state of solution which renders a reduction possible, whereupon the gaps in one columnar alphabet may be supplied from other alphabets as is shown in the example in Appendix I A 9 a.

Even though the alphabets in Appendix I A 7 b sheet 1 were taken from the number square by a certain route, the alphabets derived from one another by this method can just as well be derived by the short slide. Of course, the plain values must not be inscribed on the slide in alphabetic sequence but in a sequence obtained from the route. In the present example in Appendix I A 7 b we should have:

The plain sequence of the slide: e a r b u n g ch i t k o f s
v c z l h m p d w j x q . y „

The cipher sequence of the slide: 10 20 50 60 80 02 22 52 72 92 15 25
65 75 95 06 16 56 86 18 28 68 88 98
09 29 59 79 99

Alphabet I would be read off by setting a against 20, alphabet II with a against 52, alphabet 3 with a against 75 etc. on the slide.

The difference between a group of alphabets with random structure and one produced by the route (Duktus) is that in the latter case the alphabets can be reduced even before solution if it is possible to recognize the route and the various starting points.

However it will not always be easy to infer a route from the columnar count of a cipher text, because with columnar alphabets the number of letters of an individual alphabet which occur is subject to marked accidental variations and the possibilities of tracing a route through a number square are relatively great.

Therefore we recommend undertaking the columnar count in various number squares corresponding to the number of columns found and then marking as usable cells in all other number squares all cells occupied in any one square, as has been done in Appendix I A 9 c. It may also be worth while, as done on sheet 2 of the Appendix, to designate with a "2" the cells heavily scored in a number square, to assign the value "1" to the sparsely occupied squares, and to assign a "0" to cells not occupied in a number square, insofar as these cells may be used as is shown by a comparison with other number squares.

Hence in each number square a starting point must be fixed and for this it is best to select the most heavily scored cells in the square because it can be assumed of these cells with the greatest probability that they can be reduced one to the other. If a number square, as in our present example for alphabet II, shows two cells with equal or approximately equal scoring, then these two must both be considered as possible starting points. Correct results can only be expected if the starting cells can actually be reduced one to another.

Finally every probable or possible route must be taken out of the individual number squares, always starting with the initial cell. As a comparison of all the sequences taken out on sheet 3 of the Appendix reveals, the correct route shows a relatively high number of agreements for the values 0, 1 and 2 in comparable columns, as well as a relatively low number of contradictions such as the coming together of the value 0 and 2.

The alphabets of the table on sheet 3 of Appendix I A 8 c, on the other hand, cannot be produced by a slide because they change from column to column, due to the transposition with respect to the table on sheet 2.

Doc ID: 6592461

Nevertheless even here systematically derived alphabets are involved which can all be derived from one another with the aid of the transition sequence

c j r h u m d t g i y v l a p s o z f n q w b k x e

This sequence is called a transition sequence because it produces the transition from one alphabet to the adjacent columnar alphabet. For instance we get

from the	c	of	each	column	a	j	in	the	adjacent	column
" "	j	"	"	"	"	r	"	"	"	"
" "	r	"	"	"	"	h	"	"	"	"
" "	h	"	"	"	"	u	"	"	"	" etc.

As a comparison of the sample encipherment standing under the several encipherment tables in Appendix I A 8 c shows, it is possible in all cases where there exists such a transition sequence for the derivation of adjacent columnar alphabets, i.e. in the tables shown on sheets 1, 2 and 3, to identify plain text parallel passages - in spite of encipherment by different columnar alphabets - through the fact that their structure can be recognized by the repetition of elements standing at specific places within the plain text even though they can not be recognized by identical cipher elements. For instance, the cipher text for the plain text word "Erstbesteigung" reads, if enciphered with the table on sheet 1:

starting with column A B C etc.	vjjjcanndadqyg
" " " B C D "	wkkkdbooeberzh
" " " C D E "	xlllecppfcfsai
" " " D E F "	ymmmfdqqgdgtbj

In positions 2, 3 and 4, in positions 6 and 10, in positions 7 and 8 and in positions 9 and 11 all the cipher elements agree. The coinciding patterns of enciphermentsof the same plain text arise when enciphering with different columns if the plain text using columns progressively show certain agreements with the plain sequence which is shown in the table by the vertical coordinates.

If the starting point of the several alphabets in the transition from one column to the next moves from the top downward as on sheet 1 of the

Appendix, then certain correspondences in the letter sequence between the plain text and the plain sequence reading from the top down cause the similiarities in the cipher text just described, as is shown by a comparison of the plain sequence with the plain text word written below in various positions and also with the cipher text patterns on sheet 1 of the Appendix:

Plain sequence: abcdefghijklmnopqrstuvwxyzabcdefghijklm

Plain text:

erstbesteigung
erstbesteigung
erstbesteigung
erstbesteigung

From this figure it is clear that similiarities in the cipher text always arise when the plain text and the plain sequence have the same letters at the same intervals.

On the other hand, if the starting points of the several alphabets in their transition from one column to the next move from the bottom upward as on sheet 2 of the Appendix, then the similiarities in the cipher text occur when the plain sequence read upward shows agreement with the plain text.

If the starting points shift irregularly as on sheet 3 of the Appendix, then the plain sequence must be picked out to correspond to these degrees of displacement of the alphabet. The starting point c of the transition sequence cjrhumdt etc. is in column A on a level with plain A

" " " B " " " " " S

" " " C " " " " " I

" " " D " " " " " X.

This yields the plain sequence asixfztcmnvjbkygolreuwdqph which shows the same interval as the plain text "Asiens Revolte" for the letters asi, re and ol.e.

These similarities in the cipher text will be termed henceforth

Doc ID: 6592461

constructively similar passages or constructive parallel passages. Since these constructively similar passages agree only in their structure but not in the elements, they cannot be picked out in the usual manner by the count. But if the letters of the constructive parallel passages are designated serially 01234567890 and, omitting the first 0, letter repeats within a length of 11 letters are designated by the digits below, separating by a slash the digits for repetition of a second letter from the first digits, the following texts when converted into digits would appear as follows:

0 1 2 3 4 5 6 7 8 9 0		
w k k k a y y w d f d	=	7/123/56/80
z n n n d b b z g i v	=	7/123/56
w s e j t s x w t o s	=	7/150/48
h f x d y r w h y k y	=	7/15/480
f x d y r w h y k y r	=	40/379
x d y r w h y k y r d	=	not picked out
d y f w h y k y r d z	=	9/157/28

The numerical values thus obtained can be subjected to a count and compared with one another. This method can be used in a corresponding way for quite short or quite long constructive parallel passages, since even a repetition of the monome sequence 01234567890 beyond 0 does not lead to errors.

On the other hand, if on sheet 4 of Appendix I A 8 c the columns of a systematic Tritheim table are transposed, the result is that the individual alphabets in all the columns agree and are only cyclically displaced, so that a transition sequence from alphabet to alphabet no longer exists. Consequently plain-text parallel passages can no longer appear as constructive parallel passages (unless it be that the columnar alphabets are used repeatedly in the sequence of their transposition, which should not occur in practice, and that at the same time the plain-text parallel passages coincide in structure with the plain sequence). In the

Doc ID: 6592461

case of a Tritheim table like that on sheet 1 reduction of the individual columnar alphabets is possible even before interpretation, because the cipher secuences have an alphabetically like structure.

In the case of a Tritheim table like that on sheet 2 such a reduction of the columnar alphabets according to the principle of the short slide is possible only after interpretation.

In the case of a Tritheim table like that on sheet 3, on the other hand, a reduction of the columnar alphabets according to the principle of the short slide is not possible, even after interpretation, because the single alphabets cannot be slid in respect to one another due to the transposition of the rows.

In all three cases, however, i.e. always if a transition sequence for the derivation of adjacent alphabets is present, the constructively similar passages afford another possibility of reducing the columns before interpretation.

Since the cipher values of two constructive parallel passages have the same interval in the transition sequence as do the columnar alphabets employed for encipherment, it is possible to draw inferences from the position of the constructive parallel passage within the cipher text written out in 26 columns regarding the interval of the corresponding cipher elements of the constructive parallel passage in the transition sequence. If constructive parallel passages are present to a sufficient degree, it should be possible to reconstruct the transition sequence by their evaluation.

How this is done has been shown in Appendix I A 9 d with a plain text example of 180 elements. The plain text on sheet 1 was enciphered using the table on sheet 3 of Appendix I A 8 c. The resulting cipher text has been subjected to a count shown in a 26 column table on sheet 2 Appendix I A 9 d. At the bottom of sheet 2 Appendix I A 9 d all the constructive parallel passages in a length of 11 letters have been located consistently and these have then been marked in the cipher text.

On sheet 3 of the Appendix we have first evaluated the three constructive parallel passages with the highest ratios between length of the parallel passage and the number of cipher elements which run parallel, namely the ratios 15 : 13, 14 : 10 and 9 : 7, corresponding to our knowledge of the fact that the columnar interval of the constructive parallel passages reflects the interval in the transition sequence of the letters which run parallel. The resulting intervals between letters taken two at a time have been entered on sheet 3 of the Appendix in the vertical column a to z over against the two letters. Insofar as overlappings occurred, they have been entered on one line.

The attempt to use constructive parallel passages with less favorable ratios led in part to contradictions with the already obtained results, a sign that these constructive parallel passages are not genuine parallel passages. On the other hand an attempt was made successfully to study the elements preceding or following the already evaluated parallel passages to see whether they might also belong to the genuine repetitions in the plain text. Using all possibilities we get at least the two partial sequences

c j . h u . d . g i . v . . p . . z f . . . b k . .

r . . . . . y . l a . . o . . n q w . . x,

which can be united to form one sequence without contradiction at only one point. The sequence runs as follows:

c j r h u . d . g i y v l a p . o z f n q w b k x and embraces 22 of the 26 letters.

With the aid of this transition sequence it is possible to determine in the 26 column score on sheet 2 which cipher entries correspond to a particular plain letter. To explain this fact we have entered the number sequence 1 to 26 at the upper margin of sheet 4 to Appendix I A 9 d * and beneath this the transition sequence just reconstructed (repeated)**. On sheet 5 is shown

* This sequence 1 to 26 does not appear.
** Not actually repeated.

the decipherment table corresponding to the encipherment table in Appendix I A 8 c sheet 3 which was used in the present example but only for the two plain letters a and p. If sheet 4 is placed on sheet 5 so that the upper edge of sheet 4 is beneath Row A of sheet 5 and the digit 1 is under the column designation A i.e. as follows:

Sheet 5 to Appendix I A 9 d

ABCDEFGHIJKLMNOPQRSTUVWXYZ

A p a

1234567890123456789012345 6

Sheet 4 to Appendix I A 9 d

cjrhu.d.giyvlapozfnqwbkx.cjrhu.d.giyvlap.ozfnqwbkx

then in this position plain a results from the coordinates cipher A in column N, designated by a of the transition sequence. If sheet 4 is dropped one row on sheet 5, the letter b of the transition sequence indicates column W on sheet 5 as the column in which plain a corresponds to cipher B. In the next position plain a is then obtained from cipher C and transition value c as indicator for column A. By moving sheet 4 with a definite setting, let us say 1 on column A we can get all plain values a as the result of the coordinates

Cipher A and transition sequence value a
" B " " " " b
" C " " " " c

If sheet 4 is now laid on the count on sheet 2, Appendix I A 9 d, which has the same coordinates as the decipherment table, and is shifted in analogous fashion, then the scores corresponding to any particular plain value will be found in all the columns.

The scores taken out in the 26 different rows when sliding sheet 4 on the count square have been entered in the first line beneath the transition sequence on sheet 4 in such fashion that the count from Row A stands beneath a of the transition sequence, the count of Row B beneath b of the transition sequence, the count of Row C beneath c of the transition

Doc ID: 6592461

sequence, etc. The following rows of the consolidated counts have been produced in the same fashion save that for the second row the 2 was set against column A of the count square, for the third row the 3 of the top sequence on sheet 4.

Moreover it does not matter in what position the upper number sequence on sheet 4 stands with regard to the transition sequence beneath it because the final result is independent of this setting.

At the right of sheet 4 the scores of each row, i.e. the scores corresponding in each case to a particular plain value, have been added. These numbers yield a normal alphabet distribution so that a complete solution of the cipher text can now be achieved readily.

This proves that the constructive parallel passages in the cipher text permit of the reduction of all the columnar alphabets to a single alphabet even before interpretation.

To recapitulate, we may say that all the systematic relations between the columnar alphabets sooner or later afford a possibility for reducing the columnar alphabets, whether it be before interpretation due to

1. Derivation of the columnar alphabets according to the principle of the long slide,
2. Derivation of the alphabets according to the principle of the short slide in connection with a systematic characteristic of a cipher sequence which permits recognition of the sequence of cipher elements on the slide even before the cipher alphabets are interpreted, for instance in case of an alphabetic arrangement of the cipher sequence for monoliteral substitutions, of an arithmetic arrangement of the cipher sequence in case of number substitutions, or in the derivation from a number square by a recognizable route,
3. Derivation of columnar alphabets by means of a transition sequence in connection with a regularly progressing use of the columnar alphabets;

or be after interpretation or after partial interpretation due to

1. Derivation of the columnar alphabets according to the principle of the short slide in connection with a cipher sequence which is random or whose systematic character can only be recognized after interpretation; or
2. Other systematic characteristics which may vary according to the system.

On the other hand, if it is possible to avoid the dangers entailed by any systematic feature in the structure of the individual columnar alphabet, in its derivation from other columnar alphabets or in the sequence in which the alphabets are employed, i.e. if all the weaknesses of polyalphabetic substitution revealed in the foregoing studies can be avoided, then polyalphabetic substitution can achieve a degree of security which is greater than any other basic system affords. When properly used and when all security measures are observed, polyalphabetic substitutions can assure complete security for any amount of traffic.

Doc ID: 6592461

After solving the cipher text of Appendix I A 8 a the following is known:
Nach Lösung des Geheimtextes aus Anlage I A 8 a ist bekannt:

Klarreihe / Plain sequence	a b c d e f g h i j k l m n o p q r s t u v w x y z ä ö ü
Cäsar I / Alphabets I	75 · · 23 06 62 47 · 55 11 · · 68 34 87 38 31 · 46 54 78 43 04 64 · · 42 · ·
" II	92 · 11 02 09 68 34 87 38 31 71 · 94 78 43 · · · 59 42 83 59 · 24 · · 06 · 62
" III	09 68 34 87 38 31 71 46 94 78 43 · 64 66 59 · · · 75 24 50 23 · 62 · · 55 02 11

From the above can be formed the following fragments of the transition sequences between the alphabets:
Hieraus lassen sich folgende Bruchstücke der Übergangsreihen bilden (Ziffern der Cäsaren):

I + II :

1a : (62) (68) – 94 (42) – 06 – 09
b : 47 – 34 – 78 – 83
c : 87 – 43 – 59
d : 75 – 92
e : 55 – 38
f : 46 – 59
g : 64 – 24
h : 23 – 02

II + III :

2a : 92 – 09 – 38 – 94 – 64
b : (42) – (24) – (62) – 11 – 34 – 71 – (43) (59) – 75
c : 68 – 31 – 78 – 66
d : 02 – 87 – 46
e : 83 – 50
f : 99 – 23
g : 06 – 55

I + III :

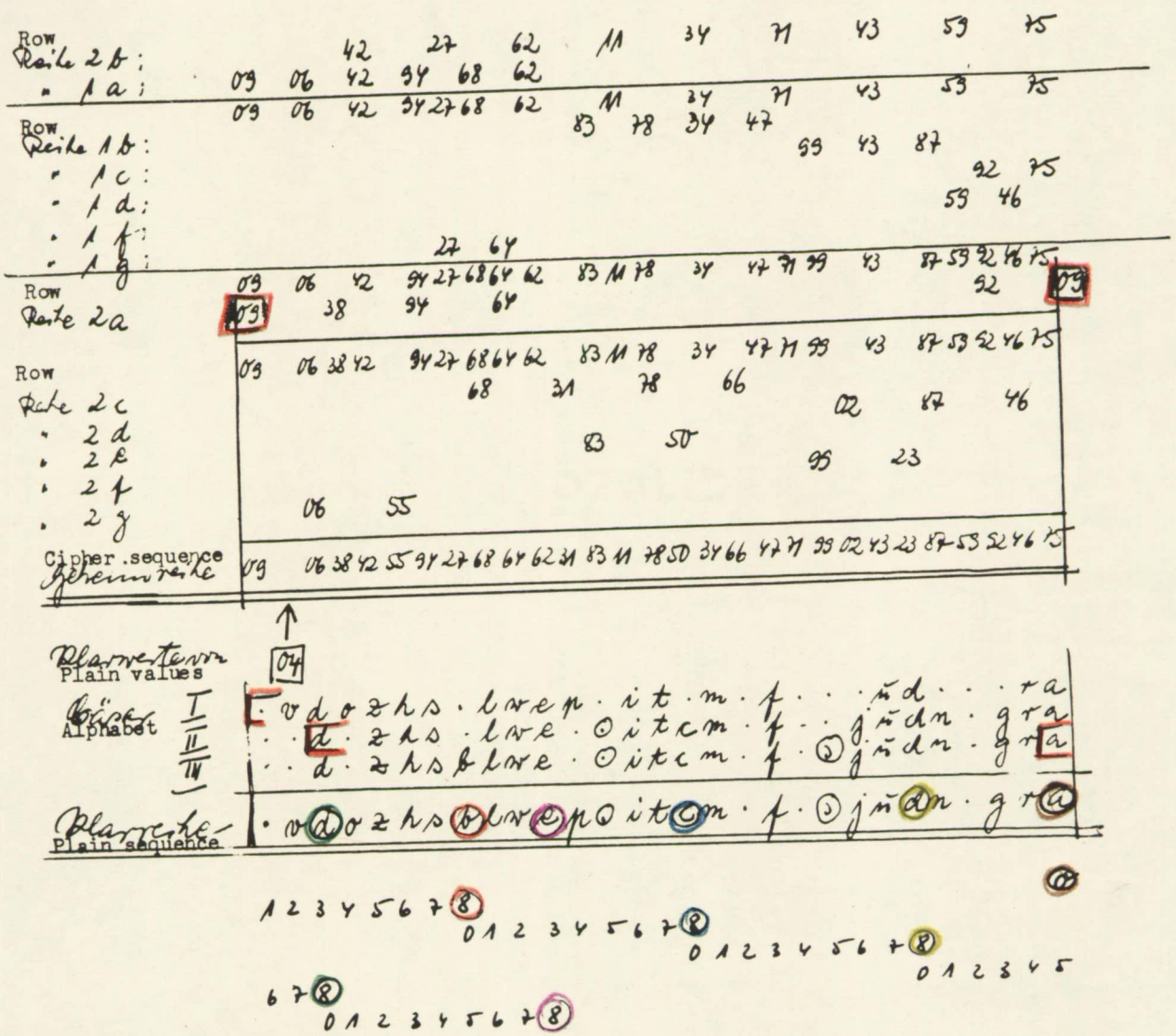
3a : 46 – 75 – 09
b : 07 – 38
c : (47) – 64 – (62) – 31
d : 44 – 71
e : (42) – 55 – 94 – (24)
f : 11 – 78 – 50
g : 34 – 66
h : (43) – 23 – 87 – (59)

IA9a

~~TOP SECRET~~

Fragment 1 a shows the substitution values 62 and 42 at an interval of 3
Bruchstück 1 a zeigt die Substitute 62 und 42 im Abstand 3
" 2 b " " " 62 . 42 . . 2

The two fragments can be united with an interval of 6 and a reversal of fragments 1 a – h
Beide Bruchstücke vereinbar im Abstand 6 und Umkehrung
der Bruchstücke 1 a – h wie folgt:



Original arrangement of:
Originalanordnung

der Klarreihe plain sequence	a b c d e f g h i j k l m n o p q r s t u v w x y z ⊙ ①
der Geheimreihe (I) cipher sequence	75 27 50 23 06 62 47 92 55 11 02 09 68 34 87 38 31 71 46 94 78 43 04 64 66 59 42 83 99
(II)	92 55 11 02 09 68 34 87 38 31 71 46 94 78 43 04 64 66 59 42 83 99 75 27 50 23 06 62 47
(IV)	09 68 34 87 38 31 71 46 94 78 43 04 64 66 59 42 83 99 75 27 50 23 06 42 47 92 55 11 02

I A 9 a – 2

~~TOP SECRET~~

Doc ID: 6592461

Original slide:
Originalschieber:

Plain sequence Klarreihe	a b c d e f g h i j k l m n o p q r s t u v w x y z ä ö ü
Geheimreihe Cipher sequence	01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28

Substitute slide: Ersatzschieber:

According to the interval which adjacent values on the substitute slide have on the original slide, the following substitute slides have been derived.

Je nach dem Abstand, den die auf dem Ersatzschieber benachbarten Werte auf dem Originalschieber haben, können folgende Ersatzschieber entstehen. Die Werte haben auf dem Originalschieber den: The values on the original slide are:

Abstand 2: Interval 2:

a c e g i k m o q s u v y ä 01 03 05 07 09 11 13 15 17 19 21 23 25 27	als Teil 1 und as part 1, and
b d f h j l n p r t v x z ö 02 04 06 08 10 12 14 16 18 20 22 24 26 28	als Teil 2 as part 2.

Abstand 3: Interval 3

a d g j m p s v y ö c f i l o r u x ä b e h k n q t w z 01 04 07 10 13 16 19 22 25 28 03 06 09 12 15 18 21 24 27 02 05 08 11 14 17 20 23 26	

Abstand 4: Interval 4

a e i m q u y 01 05 09 13 17 21 25 = Teil 1	b f j n r v z 02 06 10 14 18 22 26 = Teil 2
c g k o s w ä 03 07 11 15 19 23 27 = Teil 3	d h l p t x ö 04 08 12 16 20 24 28 = Teil 4

Abstand 5:

a f k p u ü z c h m r w ö e j o t y b g l q v ä d i n s x 01 06 11 16 21 26 03 08 13 18 23 28 05 10 15 20 25 02 07 12 17 22 27 04 09 14 19 24	

Abstand 6:

a g m s y c i o u ä d e k q w 01 07 13 19 25 03 09 15 21 27 05 11 17 23	= Teil 1
b h n t z ö d j p v x f l r u 02 08 14 20 26 04 10 16 22 28 06 12 18 24	= Teil 2

Abstand 7:

a h o v 01 08 15 22	= Teil 1	b i p w 02 09 16 23	= Teil 2
c j q x 03 10 17 24	= Teil 3	d k r y 04 11 18 25	= Teil 4
e l s z 05 12 19 26	= Teil 5	f m t ä 06 13 20 27	= Teil 6
g n u ö 07 14 21 28	= Teil 7		

Abstand 14:

a o 01 15	= Teil 1	b p 02 16	= Teil 2
c q 03 17	= Teil 3	.....	
n ö 14 28	= Teil 14		

IA 9a - 3

Doc ID: 6592461

Verhältnis von Länge des Originalschiebers und Abstand von auf dem Ersatzschieber benachbarten Werten auf dem Originalschieber bestimmt die Anzahl der Teile, aus der der Ersatzschieber besteht:

Relation of the length of the original slide and the interval on the original slide of values adjacent on the substitute slide determines the number of parts making up the substitute slide.

Länge des Originalschiebers Length of original slide	Abstand auf Ersatzschieber benachbarter Werte auf dem Originalschieber Intervals on the original slide of elements adjacent on the substitute slide.	Teiligkeit des Ersatzschiebers Number of parts of substitution slide
$28 = 1 \cdot 2 \cdot 2 \cdot 7$	$2 = 1 \cdot 2$	$2 = 1 \cdot 2$
$28 = 1 \cdot 2 \cdot 2 \cdot 7$	$3 = 1 \cdot 3$	$1 = 1$
$28 = 1 \cdot 2 \cdot 2 \cdot 7$	$4 = 1 \cdot 2 \cdot 2$	$4 = 1 \cdot 2 \cdot 2$
$28 = 1 \cdot 2 \cdot 2 \cdot 7$	$5 = 1 \cdot 5$	$1 = 1$
$28 = 1 \cdot 2 \cdot 2 \cdot 7$	$6 = 1 \cdot 2 \cdot 3$	$2 = 1 \cdot 2$
$28 = 1 \cdot 2 \cdot 2 \cdot 7$	$7 = 1 \cdot 7$	$7 = 1 \cdot 7$
$28 = 1 \cdot 2 \cdot 2 \cdot 7$	$14 = 1 \cdot 2 \cdot 7$	$14 = 1 \cdot 2 \cdot 7$
$25 = 5 \cdot 5 \cdot 1$	$4 = 2 \cdot 2 \cdot 1$	$1 = 1$
$25 = 5 \cdot 5 \cdot 1$	$5 = 1 \cdot 5$	$5 = 1 \cdot 5$
$25 = 5 \cdot 5 \cdot 1$	$10 = 2 \cdot 5$	$5 = 1 \cdot 5$

I A 9 a -4

Doc ID: 6592461

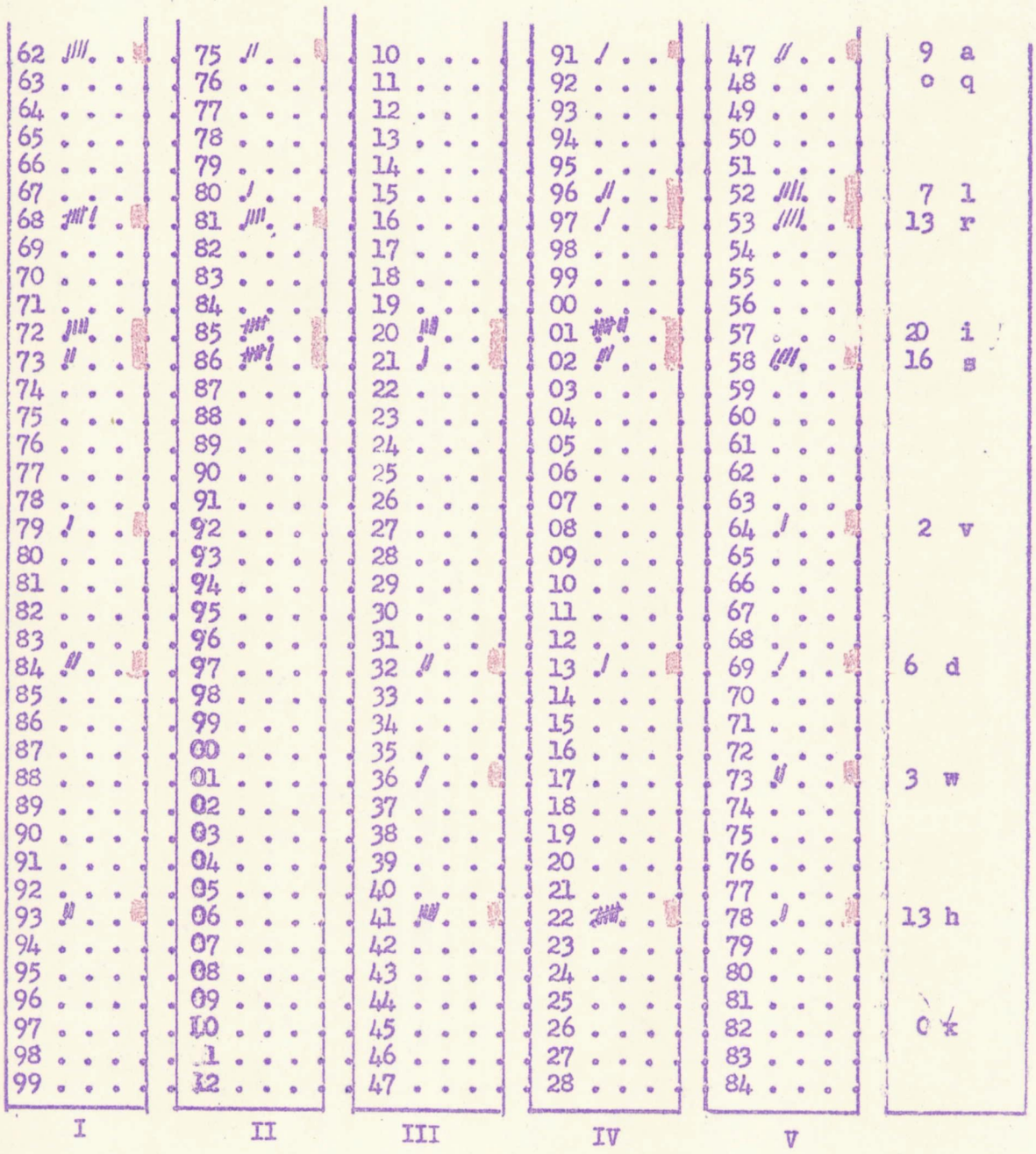
I	II	III	IV	V	
00	13	48	29	85	
01	14	49	30	86	
02	15	50	31	87	3 f
03	16	51	32	88	
04	17	52	33	89	
05	18	53	34	90	
06	19	54	35	91	1 ,
07	20	55	36	92	
08	21	56	37	93	
09	22	57	38	94	
10	23	58	39	95	
11	24	59	40	96	4 g
12	25	60	41	97	
13	26	61	42	98	
14	27	62	43	99	1 m
15	28	63	44	00	
16	29	64	45	01	
17	30	65	46	02	13 n
18	31	66	47	03	
19	32	67	48	04	
20	33	68	49	05	
21	34	69	50	06	3 .
22	35	70	51	07	
23	36	71	52	08	
24	37	72	53	09	
25	38	73	54	10	
26	39	74	55	11	5 b
27	40	75	56	12	
28	41	76	57	13	4 z
29	42	77	58	14	
30	43	78	59	15	5 r
31	44	79	60	16	
32	45	80	61	17	4 o
33	46	81	62	18	
34	47	82	63	19	7 u
35	48	83	64	20	
36	49	84	65	21	
37	50	85	66	22	o j
38	51	86	67	23	
39	52	87	68	24	
40	53	88	69	25	
41	54	89	70	26	
42	55	90	71	27	15 é
43	56	91	72	28	
44	57	92	73	29	
45	58	93	74	30	
46	59	94	75	31	10 c
47	60	95	76	32	o p
48	61	96	77	33	
49	62	97	78	34	
50	63	98	79	35	o y
51	64	99	80	36	
52	65	00	81	37	
53	66	01	82	38	
54	67	02	83	39	o k
55	68	03	84	40	
56	69	04	85	41	
57	70	05	86	42	
58	71	06	87	43	
59	72	07	88	44	
60	73	08	89	45	
61	74	09	90	46	.

(continued on next sheet)

1 A 9 b - 1

IA9b

Doc ID: 6592461



Reduction of the five alphabets from Appendix I A 8 b by sliding the values entered on strips with 100 cells until matching is achieved.

I A 9 b - 2

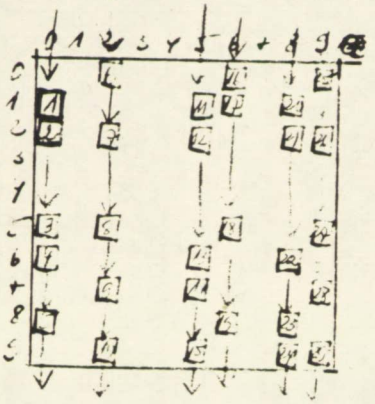
Doc ID: 6592461

TOP SECRET

The four alphabets of I A 7 b
Die vier Casaren der Anlage I A 7 b

Klardemente Plain elements	a b c d e f g h i j k l m n o p q r s t u v w x y z ä ö ü
Cäsar Alphabet I	20 60 06 52 68 10 65 22 86 72 98 15 56 18 02 25 28 29 50 75 92 80 55 88 09 73 16 53 39
II	52 96 68 75 73 22 86 65 09 95 10 16 58 28 25 26 53 50 42 18 06 15 28 95 20 80 88 60 02
III	75 06 73 18 80 65 09 86 20 28 22 88 17 50 36 58 60 42 55 29 68 16 53 02 52 15 99 32 26
IV	58 23 42 17 95 88 02 99 25 10 60 15 65 75 87 75 86 09 22 50 53 52 06 56 28 82 18 68

sind aus einem Zahlenquadrat nach einem bestimmten Schlüssel (nicht markiert) were developed from a number square



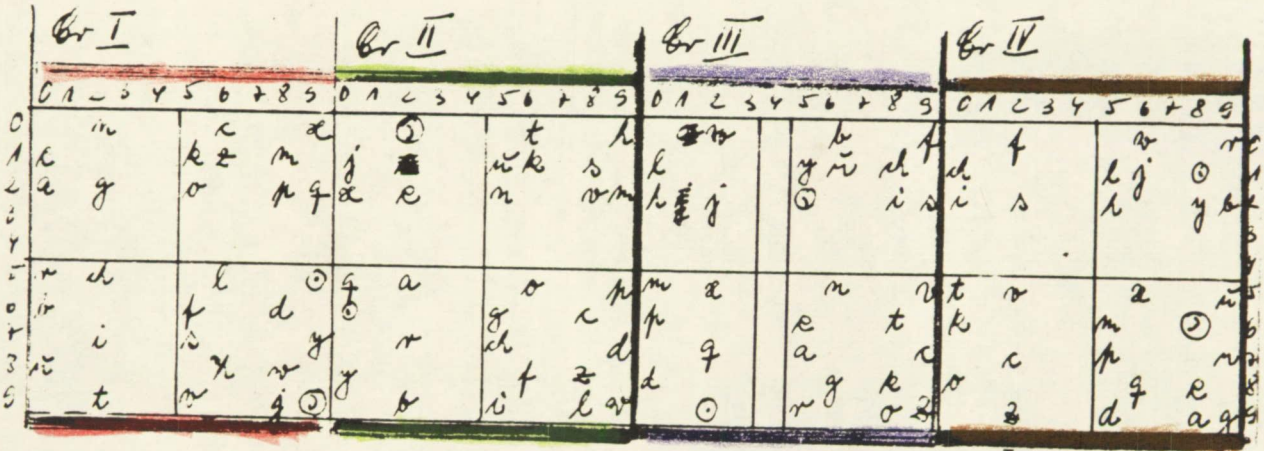
derart entwickelt worden, dass die Klarreihe
by a specific route (not marked) by inserting the plain sequence.

e a r b ü n g d i t k o f s ö c z l h m p d v j x q ö y ä

fortlaufend so in die mit 1 - 29 numerierten Felder des Quadrats eingesetzt würde, dass in
in the cells numbered 1 - 29 so that in alphabets: I e = 10; II e = 22, III e = 65, IV e = 88;

Cäsar I: e = 10, Cäsar II: e = 22, Cäsar III: e = 65, Cäsar IV: e = 88

wäre, also wie folgt:



I A 9 c - 1

125

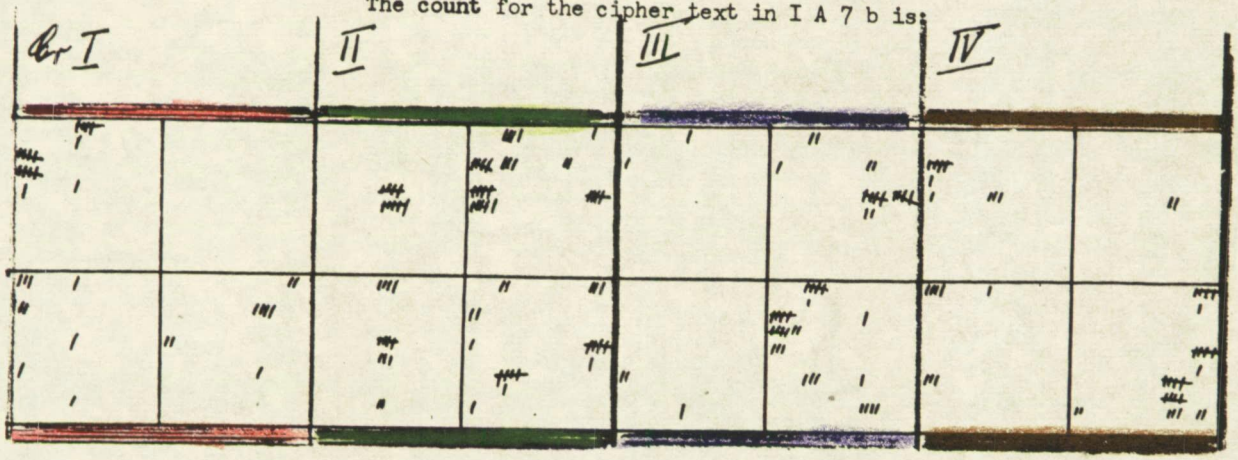
TOP SECRET

Doc ID: 6592461

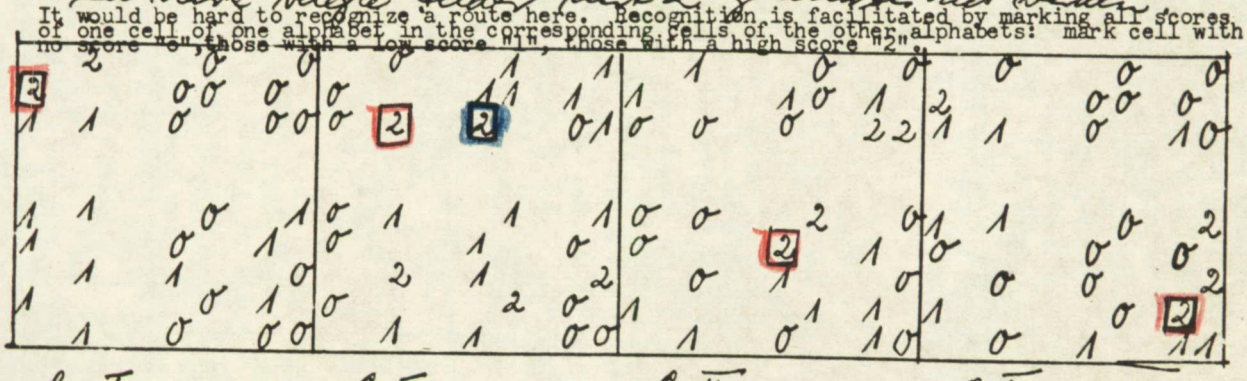
Nach der Lösung des Geheimtextes lassen sich die vier Cäsaren auf einen kurzen Schieber reduzieren (siehe Anlage I A 9b).
After solving the cipher text the four alphabets can be reduced to a short slide (see I A 9b).

Vor der Lösung des Geheimtextes ist die Reduktionsmöglichkeit nur gegeben, wenn aus der Spalten- bzw. Springcäsarenstatistik in Zahlenquadraten der Durchlauf erkannt werden kann.
Before solving of the cipher text there is a possibility of reduction only when the route can be recognized from a count of the "columnar" or "spring" Cäsars in number squares.

Die Statistik des Geheimtextes von Anlage I A 7 b ergibt folgendes Bild:
The count for the cipher text in I A 7 b is:



Einen Durchlauf daraus zu erkennen dürfte nicht schwer fallen. Erleichtert wird das Erkennen dadurch, dass alle Belegungen eines Feldes im einen Cäsar auch in den entsprechenden Feldern der anderen Cäsaren markiert worden sind: nicht belegte Felder mit 0, schwach belegte Felder mit 1 und stark belegte Felder mit 2 gekennzeichnet worden:
It would be hard to recognize a route here. Recognition is facilitated by marking all scores of one cell of one alphabet in the corresponding cells of the other alphabets: mark cell with no score "0", those with a low score "1", those with a high score "2".



~~TOP SECRET~~

Assuming that the route runs down the columns and taking the largest score as starting point of each alphabet (Alphabet [redacted] has like scores for 32 and 52) we find [redacted] following sequences:

Wird angenommen, daß der Diktus spaltenweise von oben nach unten verläuft und werden die stärksten Belegungen jedes Cäsars als Ausgangspunkte verwertet (in Br 2 Feld 32 und 52 fast stark belegt), so ergeben sich folgende Reihen:

Br I 2 1 1 1 1 2 1 1 1 0 0 0 1 0 0 0 0 0 0 0 1 0 0 0 1 0 0
IIa 2 1 2 1 1 2 1 1 1 1 1 1 2 1 0 0 0 0 1 1 1 2 0 0 0 0 0 0
IIb 2 1 1 1 1 1 2 1 0 0 0 0 1 1 1 2 0 0 0 0 0 0 2 1 2 1 1
III 2 1 0 0 0 2 1 1 2 1 1 1 0 2 0 0 0 1 0 0 0 1 1 0 0 1 0
IV 2 1 0 0 2 2 1 2 1 1 0 1 0 1 1 0 0 0 0 0 0 1 0 0 0 1 0

Verglichen mit den Reihen, die sich bei Annahme eines anderen Diktus ergeben:
If we compare this with the sequences resulting from other assumptions:

1) Annahme: Diktus jeweils von links nach rechts zeilenweise.
1) Assuming the route runs from left to right by rows:

Br I 2 = 2 0 0 0 1 1 0 0 0 1 1 0 1 1 0 1 1 1 0 1 0 1 1 1 0 0 0 2 0 0
IIa 2 = 2 2 0 1 0 1 1 1 0 1 0 2 1 2 0 2 0 1 1 0 0 0 1 1 0 1 1 1 0
IIb 2 = 2 0 1 0 1 1 1 0 1 0 2 1 2 0 2 0 1 1 0 0 0 1 1 0 1 1 1 0 2
III 2 = 2 1 0 1 0 1 1 1 1 0 1 0 1 0 0 1 1 0 1 0 0 0 2 2 0 0 2 0 0
IV 2 = 2 0 1 1 1 0 0 0 2 0 0 0 1 1 0 1 0 1 1 0 2 0 0 0 0 0 2 1 0

2) Annahme: Diktus in Schlangenlinie von 00–90, 91–01, 02–92 usw.
2) Assuming the route is serpentine: 00–90; 91–01; 02–92; etc.

Br I 2 = 2 1 1 1 1 2 1 1 1 1 0 1 0 0 0 0 0 0 0 0 1 1 0 0 0 1 0 0
IIa 2 = 2 1 2 1 1 1 1 2 1 1 1 1 2 1 0 0 0 0 0 0 2 1 1 1 0 0 0 0
IIb 2 = 2 1 1 1 1 2 1 0 0 0 0 0 2 1 1 1 0 0 0 0 0 0 2 1 2 1 1 1
III 2 = 2 0 1 0 0 2 1 1 2 1 1 1 0 0 0 2 0 1 0 0 0 1 1 0 0 0 1 0 1
IV 2 = 2 1 1 2 2 0 0 2 1 1 0 1 0 1 1 0 0 1 0 0 0 0 0 0 0 0 1 0

3) Annahme: Schlangenlinie in gelegten Spalten 00–90, 92–02, 05–95, 96–06 usw.
3) Assuming a serpentine line in the scored columns 00–90; 92–02; 05–95, 96–06; etc.

Br I 2 = 2 1 1 1 1 1 1 1 1 2 0 0 0 1 0 0 0 0 0 0 0 1 1 0 0 1 0 0
IIa 2 = 2 0 1 1 1 2 1 1 1 1 2 0 0 0 0 0 1 1 1 1 2 0 0 0 0 0 0 1 2 1
IIb 2 = 2 1 1 1 1 2 1 1 1 1 0 0 0 0 0 0 2 1 1 1 0 0 0 0 0 0 1 2 1 2 0 1
III 2 = 2 1 0 1 2 0 0 1 2 1 1 1 0 0 0 2 0 1 0 0 0 1 1 0 0 0 1 1 0
IV 2 = 2 1 1 2 2 0 0 2 1 1 0 1 0 0 1 1 0 0 0 0 0 0 1 0 0 0 0 1 0

kann die Richtigkeit dieser Diktuslinie für Br I, IIa, III und IV als erwiesen angesehen werden.
then we may regard this route for alphabets I, IIa, III and IV as correct.

~~TOP SECRET~~

Doc ID: 6592461

Plain text
Klartext

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

d i e s o r g f k t r e g i e r ü n g h o f f t a s ä

o n s r e v o l ü t i o n a e r e k a e m p f e s ä

c h z ü n ü t z e z u m a c h e n z d i e s o r g e

t r e g i e r ü n g h o f f t a t e r a ü c h d a s

p d i e s e r e v o l ü t i o n a e r e n k a e m p

f e s i c h a u f a n d e r e e r d t e i l e v o r

a s i e n a u s a u s d e h n e n w e r d e n z

180 Elemente
180 elements

Geheimtext: (Verschlüsselungstabelle in Anlage IA 8 c Seite 3)
Cipher text : (enciphering table in Appendix 1 A 8 c page 3)

Zeilenausfluss

ü ε i r p y v p r z z b y g b v t r n h o z o k k k t f j v v v o o p

t f j v v v o o p h g v h a v k k ü f c l k f ü k k n r k i v v r r s

n r k i v v o c r s ü o h l d s b t p b z j g d r a d g i i p r l p a e

g i i p r l p a e g v v g i g s x z c n c p k j x z e m c y h l p p x

e m c y h l p p x n n z d v x d o x c c v g b ü o j b g j j k d d a ü

b g j j k d d a ü i j s n v v b z v k c f ü h a g o c c c y v m l d g

c c c y v m l d g s i s n p m b t b e j z r a g

Constructive parallel passages
Konstruktive Parallelstellen

Length
Länge

Number of constructive agreements.
Anzahl der konstr. Übereinstimmungen

a . cV.	r p y v n r z z b y g b v t ±	15	13 ✓
aX. gA	k k k	3	3
bD. eG	v v o o p h g v h a v k k	14	10 ✓
bR. eV.	ü f c l k f ü k k	9	7 ✓
dM. gJ.	g i g s ü z c n c	3	4
bY. fN	k k v v k	5	3

1 A 9 d - 1

IA9d

Doc ID: 6592461

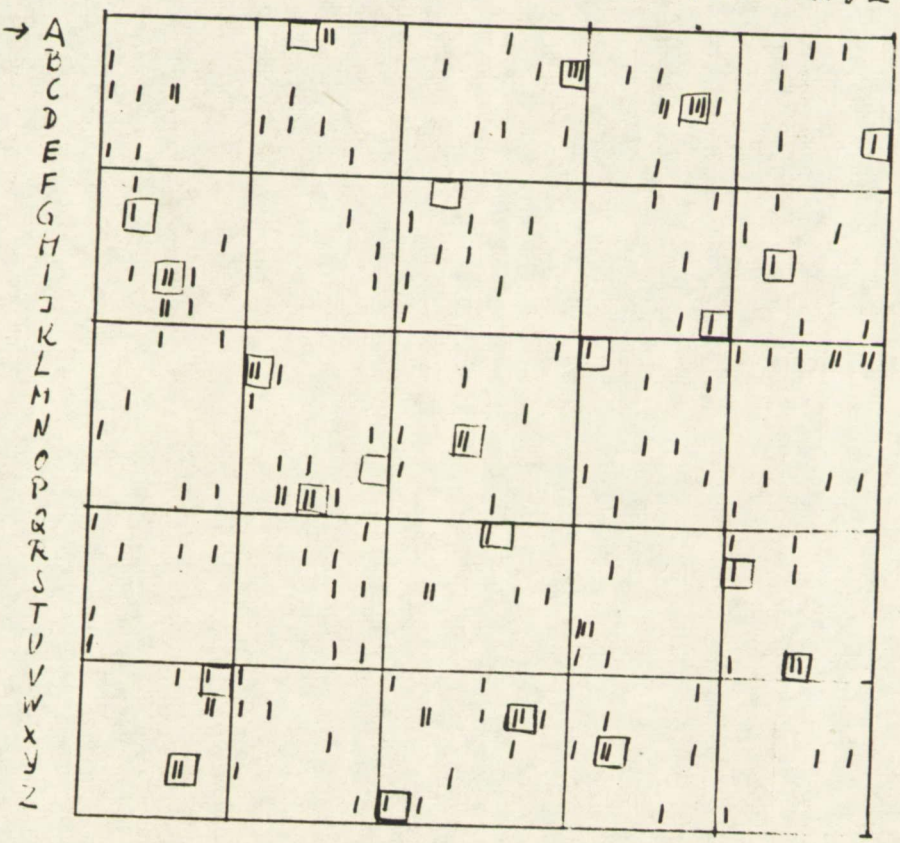
Column count of the cipher text

Spaltenstatistik des Geheimtextes

Spalte
Column

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

cipher
Geheim →



Count of constructive parallel passages.

Statistik der konstruktiven Parallelstellen

C 0/46/189a. 0/123/48a. 0/284f.

1 1/25a. 12/64/190a. 1/56/189a. 1/28/24/65d. 1/26/58/59d. 1/65/28/59d. 1/26/58/59d. 1/189c. 1/28/64/63e. 1/26/58/59e. 1/89/48/42e. 18/34f. 1/85f. 1/85f.

2 2/245/59a. 2/62d. 2/76d. 2/62f.

3 3/18/26/47a. 3/56/64d. 3/42d. 3/42d. 3/3d. 3/18c. 3/56/64c. 3/47/52e. 3/46f.

4 4/26/47d. 4/264/59e.

5 5/141-5/64a. 585/14/26d. 5/14/28/64c.

6 6/112/44d. 6/15/44d. 6/44c. 6/112/44c. 6/15/44e.

7 7/14/45/65a. 7/14/45/65c. 48/12d. 7/14/56c. 42f. 48f.

8 8/45d. 8/23/64e.

9 9/24/58a. 9/12/36a. 9/15d. 9/24/58c. 9/12/36d. 9/48d. 9/46f.

— 2 —

129

IA 9d - 2

Doc ID: 6592461

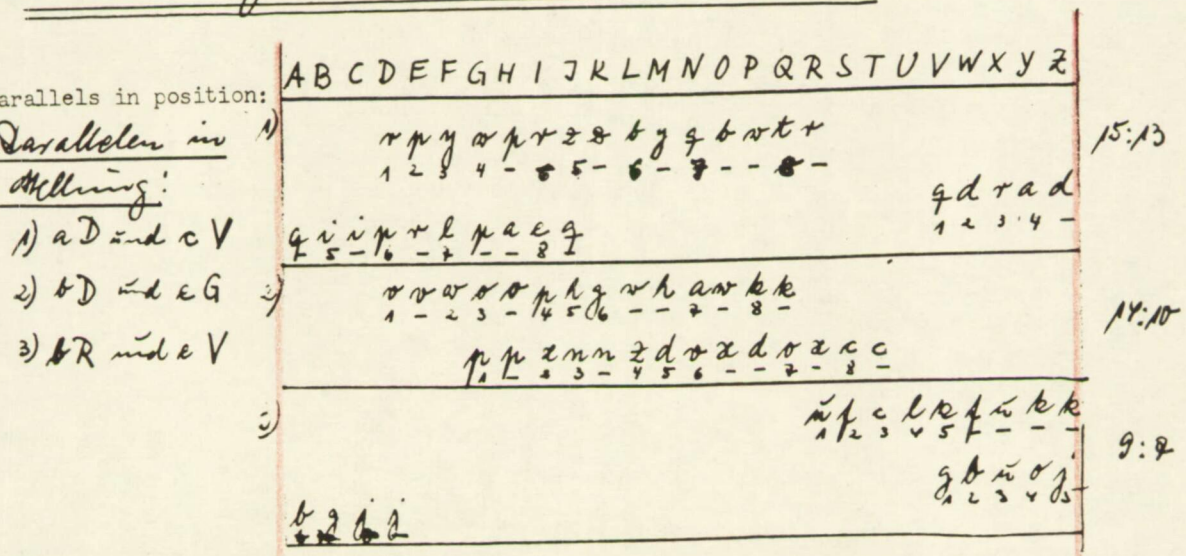
Evaluation of constructive parallel passages

Auswertung der konstruktiven Parallelstellen

Parallels in position:

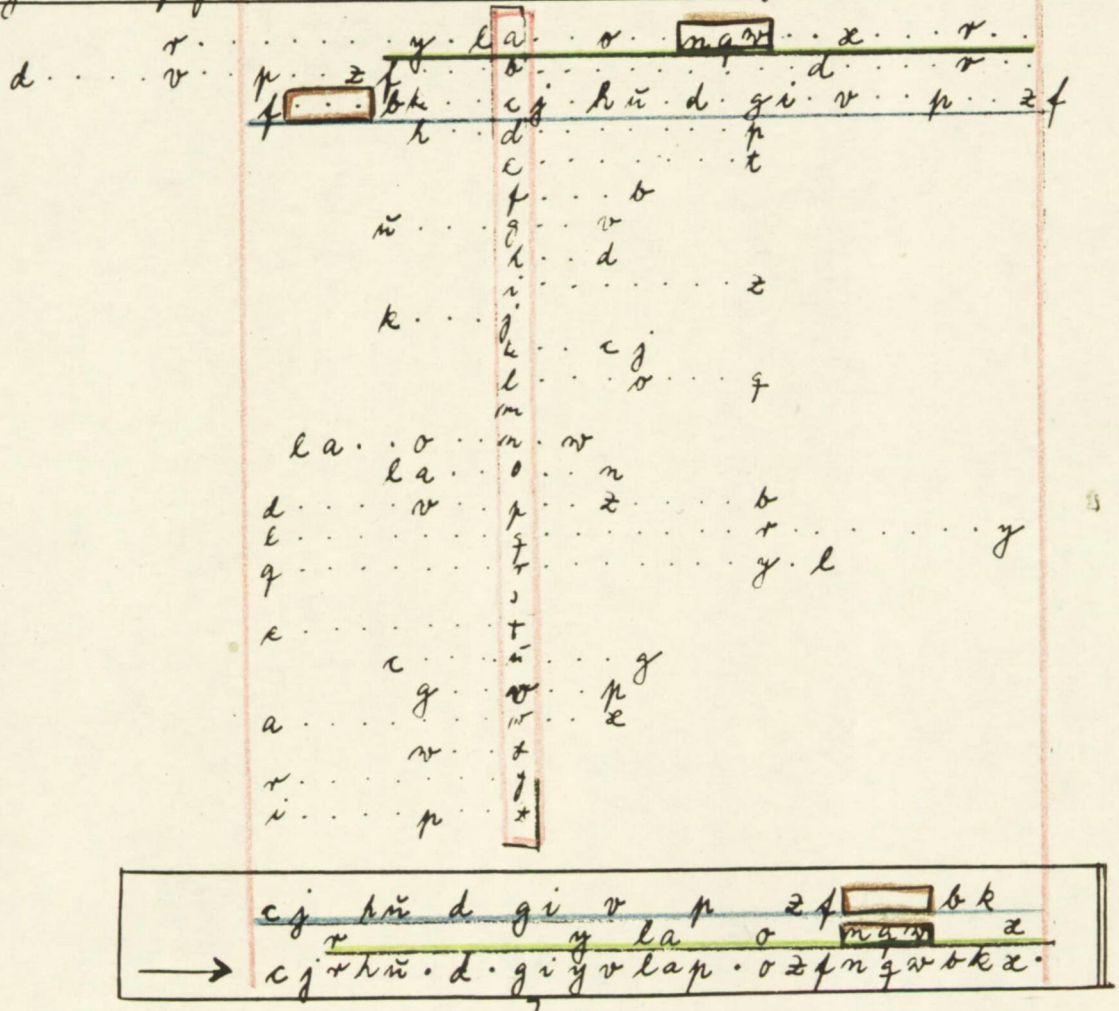
Parallelen in Stellung:

1) a D und c V
2) b D und e G
3) b R und e V



Yield the following intervals:

ergeben die folgenden Abstände auf der Übergangsreihe



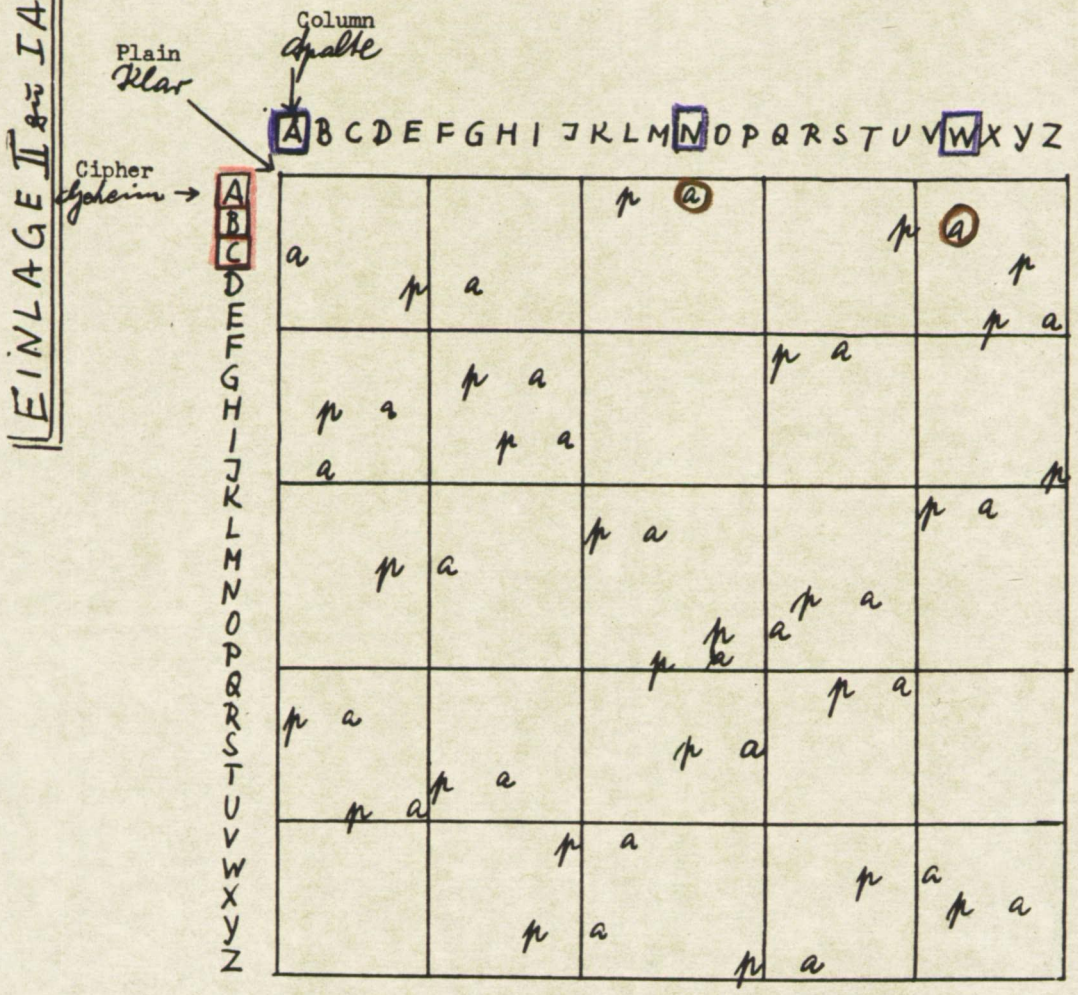
Doc ID: 6592461

EINLAGE I zu IA9d

Doc ID: 6592461

EINLAGE II zu IA9d.

EINLAGE II zu IA9d.



= deciphering table for I A 8 C - 3 partly filled.

= Entzifferungstabelle im Anhang zu I A 8 c Seite 3

TOP SECRET

Doc ID: 6592461

10. Periodic polyalphabetic substitution with selective encipherment. (Spaltencäsar mit Wahlverzifferung.)

An interesting variant of the polyalphabetic substitution, and one which introduced something completely new, was the so-called American Strip System. The innovation is found in the possibility of being able to choose the cipher text from among 25 different possibilities. This opened up an opportunity of using a definite sequence of columnar alphabets far more frequently than hitherto without endangering security.

The new idea is that a series of random alphabets inscribed on strips, slides or wheels represent the columnar alphabets. From these columnar alphabets a fixed number is put together each time in a pre-arranged sequence and the plain text to be enciphered is set against a definite row. Any of the other rows may now be selected as cipher text. If, in deciphering, this cipher text is set on the same row level with the like columnar alphabets, then one of the remaining 25 rows must yield plain text.

In this system the row may be divided one or more times so that for a one row plain text setting two half rows or three one-third rows of cipher text may be selected.

Appendix I A 10 gives an example of this method. The alphabets at the left are put together in the middle according to a key number agreed upon in advance or given in an indicator group and the plain text has been set for the top row. For encipherment half rows on the level of rows 10 and 19 have been selected. Upon setting this cipher text at the row level on the right side of the Appendix the corresponding half rows 16 and 7 yield the plain text.

When using random alphabets which cannot be reduced this method permits the use of a sequence of columnar alphabets, hence of a particular setting, as long as none of the 25 possibilities of encipherment has been used to such an extent that the intercepted cipher traffic permits solution as a polyalphabetic substitution. This condition requires the full and equal utilization of the possibilities involved in the system and a check in this regard can hardly be exercised successfully hence we must not lose sight of

Doc ID: 6592461

the fact that under these conditions the limitation of a specific sequence of columns to a definite amount of traffic is extremely difficult. Furthermore, the permissible amount of traffic depends to a high degree on whether the plain text uses stereotyped telegram beginnings or is in general of a stereotyped character or not, e.g. whether publication of part of the content entails a risk that all traffic in the same key will be capable of solution.

The question of security of columnar transpositions will have to be investigated further in connection with the study of cipher machines.

TOP SECRET

IA10

"Columnar" alphabets

1	2	3	4	5	6	7	8	9	0
h	f	e	i	k	a	g	c	a	d
q	p	q	a	g	m	i	d	e	h
i	u	l	p	z	t	h	m	f	b
e	a	p	o	p	l	k	j	v	m
o	t	y	x	u	v	r	w	z	a
j	m	v	j	w	p	s	k	g	q
r	z	f	z	a	q	m	o	y	l
s	e	z	h	t	b	d	u	o	p
d	r	d	y	b	k	e	l	n	v
n	l	n	n	l	c	j	e	q	y
f	x	s	u	o	w	t	b	p	e
z	b	g	k	h	o	c	s	r	j
g	q	x	b	j	u	f	a	m	z
x	g	k	q	q	r	v	f	b	n
w	w	r	g	i	d	x	n	l	o
a	k	c	v	x	j	b	t	w	f
y	s	m	c	m	y	u	p	k	t
k	j	b	r	v	e	p	y	c	u
p	v	w	f	c	i	y	g	x	g
v	c	i	w	e	n	q	z	s	x
u	d	o	l	r	f	z	q	j	s
b	n	t	s	y	z	a	h	u	v
l	h	a	d	n	s	w	x	t	i
m	i	u	m	s	g	o	r	h	c
t	y	h	t	d	x	n	v	i	r
c	o	j	e	f	h	l	i	d	k

Sample encipherment

	Numerical key	5	3	2	0	4	1	6	9	8	7	0	4	3	8	6	1	7	9	2	5
	Plain text	n	a	c	h	v	i	o	h	t	s	n	d	i	e	n	s	t	m	e	l
0		s	u	d	b	f	e	w	i	p	j	o	m	o	b	f	d	c	b	r	o
1		d	h	n	m	v	o	o	d	y	t	f	t	t	s	z	n	f	l	l	h
2		f	g	h	a	l	j	u	a	g	c	t	e	a	a	s	f	v	v	x	j
3		k	e	i	q	s	r	r	e	z	f	u	i	u	f	g	z	x	k	b	q
4		g	q	y	l	d	s	d	f	q	v	g	a	h	n	x	g	b	c	q	i
5		z	l	o	p	m	d	j	v	h	x	x	p	j	t	h	x	u	x	g	x
6		p	p	f	w	t	n	y	z	x	b	s	o	e	p	a	w	p	s	w	m
7		u	y	p	y	e	f	e	g	r	u	v	x	q	y	m	a	y	j	k	v
8		w	v	u	e	i	z	i	y	v	p	i	j	l	g	t	y	q	u	s	c
9	Cipher text	a	f	a	j	a	g	n	o	i	y	c	z	p	z	l	k	z	t	j	e
10		t	z	t	z	p	x	f	n	c	q	r	h	y	q	v	p	a	h	v	r
11		b	d	m	n	o	w	z	q	d	z	k	y	v	h	p	v	w	i	c	y
12		l	n	z	o	x	a	s	p	m	a	d	n	f	x	q	u	o	d	d	n
13		o	s	e	f	j	y	g	r	j	w	h	u	z	v	b	b	n	a	n	s
14		h	g	r	t	z	k	x	m	w	o	b	k	d	v	k	l	l	e	h	d
15		j	x	l	u	p	p	h	b	k	n	m	b	n	i	c	m	g	f	i	f
16	Cipher text	q	k	x	g	y	v	a	l	o	l	a	q	s	c	w	t	i	v	y	k
17		i	r	b	x	n	u	m	w	u	g	q	g	g	d	o	c	h	z	o	g
18		x	c	q	s	u	b	t	k	l	i	l	v	x	m	u	h	k	g	f	z
19		m	m	g	v	k	l	l	c	e	h	p	c	k	j	r	g	r	y	p	p
20		v	b	w	i	b	m	v	x	b	k	w	r	r	w	d	i	t	v	u	u
21		c	w	k	c	q	t	p	s	s	r	y	f	c	k	j	e	m	n	a	w
22		e	i	s	r	g	c	q	j	a	s	e	w	m	o	y	o	d	q	t	a
23		r	o	o	j	k	v	h	b	u	f	m	j	l	b	u	e	j	e	p	m	t
24		y	t	v	d	c	q	k	t	n	d	x	s	w	l	i	r	j	r	z	b

Sample decipherment

	Numerical key	5	3	2	0	4	1	6	9	8	7	0	4	3	8	6	1	7	9	2	5
	Cipher text	a	f	a	j	a	g	n	o	i	y	l	v	x	m	u	h	k	g	f	z
0		t	z	t	z	p	x	f	n	c	q	p	c	k	g	r	q	r	y	p	p
1		b	d	m	n	o	w	z	q	d	z	w	r	r	w	d	i	s	o	u	u
2		l	n	z	o	x	a	s	p	m	a	y	f	c	k	j	e	m	n	a	w
3		o	s	e	f	j	y	g	r	j	w	e	w	m	o	y	o	d	g	t	a
4		h	g	r	t	z	k	x	m	w	o	j	l	b	u	e	j	e	p	m	t
5		j	x	l	u	h	p	h	b	k	n	z	s	w	l	i	r	j	r	z	b
6	Plain text	q	k	x	g	y	v	a	l	o	l	n	d	i	e	n	s	t	m	e	l
7		i	r	b	x	n	u	m	w	u	g	o	m	o	b	f	d	c	b	r	o
8		x	i	q	s	u	b	t	k	l	i	b	t	t	s	z	n	f	l	l	h
9		m	m	g	v	k	l	l	c	e	h	t	e	a	a	s	f	v	w	x	j
10		v	b	w	i	b	m	v	x	b	k	u	i	u	f	g	z	x	k	b	q
11		c	w	k	c	q	t	p	s	s	r	x	p	j	t	h	x	u	x	g	x
12		e	i	s	r	g	c	q	o	a	s	s	o	e	p	a	w	p	s	w	m
13		r	o	j	k	v	h	b	u	f	m	v	x	q	y	m	a	y	j	k	w
14		y	t	v	d	c	q	k	t	n	d	i	j	l	g	t	y	q	u	s	c
15	Plain text	n	a	c	h	r	i	c	h	t	e	c	z	p	z	l	k	z	t	j	e
16		s	u	d	b	f	e	w	i	p	g	r	h	y	q	v	p	a	h	v	r
17		d	h	n	m	v	o	o	d	y	t	k	y	v	h	p	v	w	i	c	y
18		f	j	h	a	l	j	u	a	g	c	d	n	f	x	q	u	o	d	d	n
19		k	e	i	q	s	r	r	e	z	f	l	u	z	r	b	b	n	a	n	s
20		g	q	y	l	d	s	d	f	s	v	b	k	d	v	k	l	l	e	h	d
21		z	l	o	p	m	d	j	v	t	x	m	b	n	i	c	m	g	f	i	f
22		p	p	f	w	t	n	y	z	x	b	a	q	s	c	w	t	i	v	y	k
23		u	y	p	y	e	f	e	g	r	u	g	a	h	n	x	g	b	c	q	i
24		w	v	u	e	i	z	i	y	v	p	q	g	g	d	o	c	h	z	o	g
25																					

IA 10

135

TOP SECRET

Doc ID: 6592461

Doc ID: 6592461

11. The code

As already mentioned in connection with polyalphabetic substitutions there existed for the further development of cryptographic work the possibility of extending the use of variants and the introduction of syllables already encountered in the syllable substitution so that instead of systems with one or two letters or digits more would be employed.

For these 3, 4 and 5-place systems the name code has been introduced although there is no basic difference between the substitution alphabet and the code but merely one of degree. Both in the code and in the substitution the individual elements of the plain language are replaced by cipher elements in the sequence natural to the language. In the substitution the individual letters and digraphs and even syllables and articles are provided with cipher elements while in the code substitute values are provided for the single letters, digraphs and trigraphs as so-called spelling groups but also for words, groups of words or phrases and sentences, and likewise for place names and personal names.

These extensive codes aim both to increase the security of this cryptographic system as far as possible and also to reduce the length of the cipher text in comparison to that of the plain text as greatly as possible and thus save on telegraph and cable charges.

The size of codes varies greatly according to their structure and the number of places in the code groups. If number codes are used we may get with

3-digit groups	10^3 =	1000 groups
4-digit groups	10^4 =	10,000 groups
5-digit groups	10^5 =	100,000 groups

Any greater number of places is not usual because with 100,000 groups we already have a very extensive code book of some 1,000 pages which is capable of meeting all demands. On the other hand, when letter codes are involved the theoretical size, using the 26 letter alphabet, is for

Doc ID: 6592461

3-letter groups 26^3 = 17,576

4-letter groups 26^4 = 456,976

5-letter groups 26^5 = 11,881,376 groups.

It is hardly necessary to mention the fact that the theoretical limit is virtually never used in the case of 4- and 5-letter codes.

The groups of these letter codes often show a systematic structure which on the one hand reduces the number of possible groups and on the other hand affords certain advantages in that the groups are pronounceable or that in case of errors in composition or transmission the proper group can be reconstructed more readily so that inquiries may be avoided in case of slight garbles in the encoded text (e.g. when sent by radio) without running the risk of a false reconstruction which might give rise to misunderstandings or errors.

To secure pronounceable groups, it is well to observe a definite alternation of vowels and consonants within the group. If we designate the vowels by v and the consonants by c and note the number of different vowels or consonants which can occur at a given position within the group, we get, for instance, the following possibilities:

1. c v c v or v c v c
   20 5 20 5 5 20 5 20 = a 4-letter code with 100 pages each with 100 lines which is equal to a 4-digit code of 10,000 groups

2. c v c v
   20 6 20 6(y counts as 6th vowel) = a 4-letter code with 120 pages each with 120 lines and a total of 14,400 groups.

Doc ID: 6592461

3. c v c v
20 5 20 5
v c v c
5 20 5 20
= a 4-letter code of 200 pages each with 200 lines and a total of 40,000 groups.

4. v c v c v
5 20 5 20 5
= a 5-letter code of 500 pages each with 100 lines or a total of 50,000 groups.

5. v c v
5 20 5
c v
20 5
v c
5 20
= a 5-letter code of 500 pages each with 200 lines or a total of 100,000 groups

6. c v c v c or c v c c v
20 5 20 5 20 20 5 20 20 5

or c v c
20 5 20
v c
5 20
c v
20 5
= a 5-letter code with 2,000 pages of 100 or of 200 lines making a total of 200,000 or 400,000 groups.

In this way 4- and 5-place codes of any size and for any purpose can be produced.

On the other hand the systematic feature of the group structure may consist in associating the numerical values to the individual letters of which the group is composed and constructing the groups so that their cross sums always give a definite value. Since in this case one element in the group serves as control element, which is of necessity the complement to the cross sum of the other elements, such a 4-place system would only have the extent of a 3-place code and a 5-place only the extent of a 4-place code.

The simplest method of doing this would be to equate a = 1, b = 2, c = 3 ... z = 26 and have the cross sum of the group always 26, in which case sums over 26 would again start with one. Then, for example, with a 4-letter code the following group formations would be possible:

aaaw = 01 01 01 23 = 26
aabv = 01 01 02 22 = 26
aacu = 01 01 03 21 = 26
....
....
....
aawa = 01 01 23 01 = 26
aaxz = 01 01 24 26 = 26
aayy = 01 01 25 25 = 26
aazx = 01 01 26 24 = 26

abav = 01 02 01 22 = 26
abbu = 01 02 02 21 = 26
....
....
....
abzw = 01 02 26 23 = 26

If the transmitted group should then read g h o s instead of the correct group g h r s = 07 08 18 19 = 26, then no such group would exist in the code because the cross sum 07 08 15 19 = 23. Assuming that only one mistake is to be found in the group, the correct group could read:

j h o s = [10] 08 15 19 = 26

g k o s = 07 [11] 15 19 = 26

g h r s = 07 08 [18] 19 = 26 or

g h o v = 07 08 15 [22] = 26

Assuming always that there is only one garble in the transmission of the erroneous group, the cross sum will essentially limit the number of possible correct groups. Without the control letter the group would have been 3-place and would have read g h r or g h o; in this case instead of 4 groups we should have to select from 26 + 26 + 25 = 77 possibilities.

On the other hand if a transmission error consists in the transposition of two elements of the group, for instance if the correct group g h r s is transmitted as h g r s, then the control letter fails of its purpose since the cross sum is the same in both cases.

However the group structure can be arranged so that the control values will also indicate transposition of correct elements within the group. In this case it is necessary that the letters have different values according to their positions within the group. On the top of sheet 1 of Appendix I A 11 a is a sample table where the value of a letter in the first position of the group is doubled in the second position, trebled in the third position, quadrupled in the fourth position and quintupled in the fifth position, beginning with 1 again whenever 29 is exceeded.

Doc ID: 6592461

To round out the system, rows I, II, III, IV and V for the setting of a letter in the 1, 2, 3, 4, and 5th position within the group have been extended 3 values beyond z . Consequently the prescribed cross sum of the groups is 29.

If the transmitted group reads, for example, c l s b v = 03 24 28 08 23 = 28, instead of the correct group d l s b v = 04 24 28 08 23 = 29, then assuming that only one element is false, the correct group can only read:

d l s b v = 04 24 28 08 23 = 29 or

c l s x v = 03 24 28 09 23 = 29.

In this case no other potentially correct groups can be formed because in the second, third, and fifth positions of the group no letters can be found with a value one greater than that of the transmitted letter.

If the table is arranged not according to letters but according to numerical values, i.e. if it appears in the form shown at the bottom of sheet 1 of the Appendix, then those values can be read off which may be used to replace a garbled value.

In the above example where the transmitted group c l s b v showed the cross sum 28 it would be necessary to replace one element at a time by another with a value greater by one so that the group will attain the correct cross sum 29. From the table we get for the first element "c" from row I "d", for the second element "l" from row II a - . For the third element "s" in row III a -, for the fourth element "b" in row IV an "x" and for the fifth element "v" from row V a -. Hence the correct group could be d l s b v or c l s x v.

If the transmission error consists in the transposition of two adjacent elements, for instance if instead of d l s b v the group l d s b v is transmitted, this error is likewise revealed by the cross sum. While the cross sum of d l s b v = 04 24 28 08 23 = 29, the cross sum for l d s b b = 12 08 28 08 23 = 21. The cross sum is therefore too low by the amount of the interval from d to l in row I of the table arranged by numerical values, namely 8.

Doc ID: 6592461

Even when the elements have been transposed in position II and III, III and IV or IV and V instead of I and II, the difference from the prescribed cross sum corresponds to the interval between the inverted elements in the alphabet. Thus the difference between d s l b v = 04 09 07 08 23 = 22 and the proper cross sum is 7, and the interval from l to s is also 7.

But transpositions of elements not adjacent in the group are also revealed, only the difference with respect to the cross sum is double the interval between the interchanged letters of the alphabet if the transposed elements are two apart, thrice the interval if the elements are three apart and four times if the interval within the group is four. On the other hand if the interval between the interchanged letters is computed not in the alphabet but on the row I, II, III or IV of the table, according to whether the interchanged elements have an interval of 1, 2, 3 or 4 in a group, then the difference with respect to the cross sum indicates the interval of the interchanged letters in the appropriate row. Thus if instead of d l s b v the transmitted group reads b l s d v = 02 24 28 16 23 = 6, then the element d and b corresponding to their interval 3 within the group will be at an interval of 23 in row III of the table.

This table can also be used in the form of a 5-part slide to determine the correct group. This is illustrated on sheet 2 of the Appendix. If the elements of the falsely transmitted code group are set up on slides I, II, III, IV and V against column 0, then in the column indicated by the complement to the cross sum of the group with reference to the proper cross sum 29 can be read off the values which could stand as correct element in positions 1 to 5 of the group.

If on the other hand the first element of the group is set up with slides I, II, III and IV set at the 0 column, the column indicated by the cross sum of the group will show on the slides those letters which - if they should stand in the 2nd, 3rd, 4th, or 5th position in the group - would give the correct cross sum if transposed with the element set up.

In other words: if one of the slides set contains in the column involved a letter which is contained in the group at that interval, then interchanging this letter with the letter set up will yield the correct cross sum. The same experiment must then be made by setting the second element of the group on slides I, II, and III, the third element on slides I, and II, and the fourth element on slide I, in order to complete the study.

By setting up the slides in this way all those groups can be read off which might stand in place of the garbled group, insofar as we assume that one element of the group is garbled or that two elements have been interchanged. Thus with the group structure based on the cross-sum 29 it results that any single error in transmission of the group and also a transposition of two elements will be indicated by a deviating cross-sum and that the difference between this and the standard cross-sum will at the same time give clues to the error.

Just as in the case of the substitution alphabet, it is possible with a code to have systematic or unsystematic [random] assignment of meanings to the groups and to use one or more groups for any meaning.

If the code is alphabetic, then when the plain text meanings are arranged alphabetically the code groups will also stand in alphabetic or arithmetic order depending on whether it is a letter or number code. In this case the same code may be used for both encipherment and decipherment. If on the other hand the code is unsystematic in structure, then one part must be prepared with the plain concepts in alphabetic order for encipherment and another part with the code groups in systematic order for decipherment. The increased labor involved and the correspondingly higher costs explain why one-part codes are relatively numerous.

The enciphering part of a code with the plain concepts arranged alphabetically is often divided by subjects. For instance there are frequently special sections for spelling groups, numbers, auxiliary verbs, geographic names, personal names etc., in addition to the main section for words and sentences.

Words, concepts, phrases and punctuation marks occurring frequently in plain language may be assigned several groups. Depending upon the size of the code, variants may be assigned plentifully so that from 30 to 50

Doc ID: 6592461

different code groups for a single plain concept are no exception. Of course one must not entertain any illusions regarding the very relative value of a large number of variants.

In some cases the question of variants is handled not by assigning several code groups to a single plain concept but by associating several plain concepts to one code group. Thus it is possible for each group to represent

1. A word or phrase,

2. A proper name - geographic or personal,

3. A spelling group, single element, number etc.

When the second or third meaning is to be taken, this can be shown by special indicator groups, in case these are not dispensed with because the appropriate meaning is generally obvious from the context.

Finally the code may be used with groups of varying length so that, for instance, part of the page designations will be 1-place or 2-place, while the other part will be 2-place or 3-place.

Regarding the security of a code against unauthorized decryption it is obvious that a single message affords no possibility of solution. However it will generally suffice to show that the cryptographic system involved is a code with groups of such and such a length. If several messages are available, each individual message must be studied, using a count or some other method, to determine whether it belongs to the same code. This must be continued until the indicator groups have been recognized to such an extent that they can be used for identification.

If it is a letter code, the group structure must first be determined in order to prepare a corresponding code book for the total count of all messages belonging to the code. This book provides for each group a separate cell or line where the position index for each occurrence of the group can be entered.

After relatively few messages have been subjected to a count, frequent groups will begin to stand out as such. From the distribution of these frequent groups within the code it is usually possible to tell whether a

one-part or two-part code is involved. For instance, if the basic language is French, then with a one-part code the groups for a and à , for de, de l' and de la, for á l' and á la, etc. will attract attention because they come close together, as will groups signifying references or numbers.

If it is a one-part code, then the number of unused groups between the frequently used groups will afford important clues to the potential meanings. If these clues are taken in connection with the frequency of the groups and the position of the group in the code text and in relation to other frequent groups, it is easy to break into a one-part code with relatively little traffic. As an example we will use the following actual case. For a one-part four-letter code with unsystematic group structure and a total of about 40,000 groups which had recently appeared there were available just under forty messages of medium length. After the group structure had been determined and a blank code had been prepared, all the messages were solved completely within a fortnight. It is true that the traffic in this case had fairly uniform content.

From this example it can be seen that even in favorable cases the energy required to produce a code of such size bears no relation to the results if the code is intended as a cryptographic system and not merely as a means of reducing telegraph charges.

If on the other hand a two-part code is involved, then obviously a greater amount of traffic is necessary before one can start with the interpretation. Moreover the interpretation of such a code makes greater demands on the worker's intuition and ability to put two and two together. But even when a two-part code is of considerable size and has many variants, the inferences to be drawn from the position of frequent groups and from the inevitable occurrence of parallel passages within the code text are so extensive that, although the first attempts at interpretation will be groping and cautious, after four to six weeks or when a total of one hundred to two hundred messages of average length have accumulated, some short messages can be read in full while in the case of the other messages some guess can be made as to the possible

Doc ID: 6592461

contents. Once this stage has been reached, the rest of the work usually progresses with gigantic strides. After a few more weeks the majority of the messages can already be interpreted with fair certainty.

In this work it will be well to enter the position indices of all groups in the blank code until the interpretation of a group has been achieved with absolute certainty. After that the meaning originally entered in pencil will be entered in ink to indicate that there is no longer any question that a synonym might stand in this position.

All that can certainly be gained with a two-part code is then a certain delay in reading during the first two or three months it is in use. After that the difficulties of breaking into the code will have been overcome by the unauthorized decrypter to such an extent that any delay in current reading does not occur or is no longer of importance.

The reason why even a two-part code can be solved is found in the fact that the encoded text always reveals the frequencies of the plain language. Even extensive use of variants does not alter this. Even the use of special indicator and camouflage groups, such as "read instead of the following group the tenth group following in the code" or "at this point read the tenth group of this message" can - if carried out consistently - merely prevent the occurrence of parallel passages within a single message. It cannot prevent the occurrence of parallel passages in messages sent at different times. Such means can, to be sure, somewhat delay solution but they are not able to give the system any increased security.

Consequently, when a code is not intended to shorten the cipher text in comparison to the plain text and possibly to serve at the same time as the basis for superencipherment, the great expense involved in the production of the code is out of all proportion to its practical value.

A glance back over all the substitution systems leads to the basic conclusion that security cannot be attained by a greater expansion of the system, unless it be that one is ready to disregard any ratio between expense and usefulness. The only proper course with substitution systems has proven to be the use of a multiplicity of systems with a minimum of traffic

Doc ID: 6592461

in the individual system, such as is possible with polyalphabetic substitution. With this, however, all the possibilities of the substitution systems are exhausted.

Doc ID: 6592461

TOP SECRET

EVALUATION TABLE FOR 5-LETTER GROUP WITH THE CROSS-SUM 29
(In case of sums above 29, start again with 1 following 29)

Value of the elements	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	-	-	0
In position I	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29
" " II	02	04	06	08	10	12	14	16	18	20	22	24	26	28	01	03	05	07	09	11	13	15	17	19	21	23	25	27	29
" " III	03	06	09	12	15	18	21	24	27	01	04	07	10	13	16	19	22	25	28	02	05	08	11	14	17	20	23	26	29
" " IV	04	08	12	16	20	24	28	03	07	11	15	19	23	27	02	06	10	14	18	22	26	01	05	09	13	17	21	25	29
" " V	05	10	15	20	25	01	06	11	16	21	26	02	07	12	17	22	27	03	08	13	18	23	28	04	09	14	19	24	29

The above evaluation table arranged by numerical values:

	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	0
Position I	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	-	-	-
" II	o	a	p	b	q	c	r	d	s	e	t	f	u	g	v	h	w	i	x	j	y	k	z	l	-	m	-	n	-
" III	j	t	a	k	u	b	l	v	c	m	w	d	n	x	e	o	y	f	p	z	g	q	-	h	r	-	i	s	-
" IV	v	o	h	a	w	p	i	b	x	q	j	c	y	r	k	d	z	s	l	c	-	t	m	f	-	u	n	g	-
" V	f	l	r	x	a	g	m	s	y	b	h	n	t	z	c	i	o	u	-	d	j	p	v	-	e	k	q	w	-

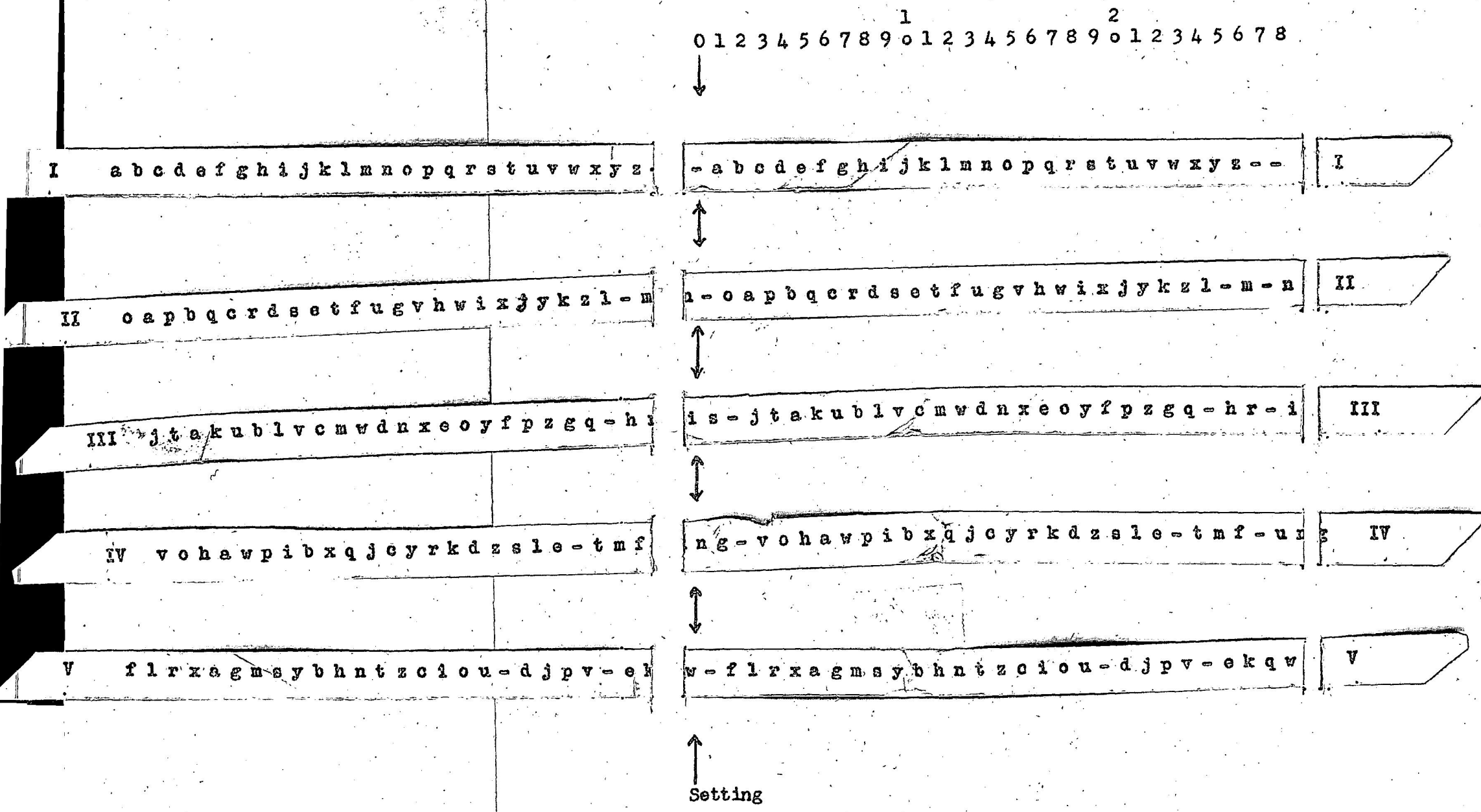
Appendix I A 11 a -1

TOP SECRET

TAB

Doc ID: 6592461

Slide to determine matching elements



Example 1:

The transmitted group e l s b v cross sum 1

Setting of	e	on	slide	I	gives	in	column	28	(29 - 1)	= d
"	"	l	"	II	"	"	"	"		= z
"	"	s	"	III	"	"	"	"		= i
"	"	b	"	IV	"	"	"	"		= i
"	"	v	"	V	"	"	"	"		= p

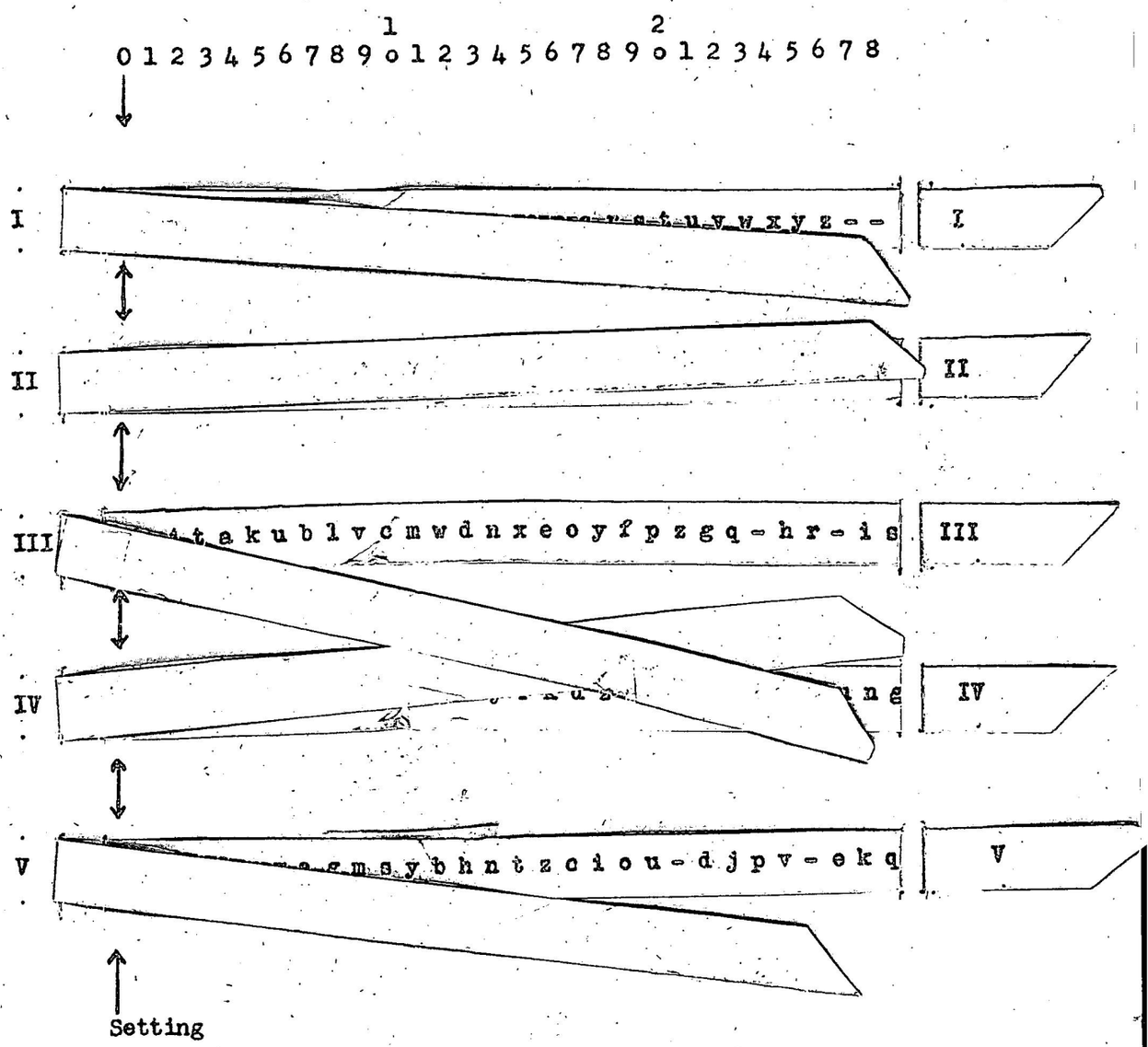
Groups with the cross sum 29:

d l s b v, e z s b v, e l i b v, e l s l v, e l s b p

I A 11 a - 2

Doc ID: 6592461

Slide to determine matching elements



Example 1:

The transmitted group e l s b v cross sum 1

Setting of	e	on slide	I	gives in	column	28 (29 - 1)	=	d
"	"	l	"	"	II	"	"	"	"	=	z
"	"	s	"	"	III	"	"	"	"	=	i
"	"	b	"	"	IV	"	"	"	"	=	i
"	"	v	"	"	V	"	"	"	"	=	p

Groups with the cross sum 29:

d l s b v, e z s b v, e l i b v, e l s i v, e l s b p

I A 11 a - 2

Furthermore the setting:

Strip	I	II	III	IV	yields in	I	II	III	IV
0 =	e	e	e	e		1 =	f	ɟ	ɸ	-
0 =	l	l	l			1 =	ɱ	-	v	
0 =	s	s				1 =	ɟ	ɸ		
0 =	b					1 =	ɸ			

Hence the group c v s b l yields the cross sum 29.

Example 2

Transmitted group d l v b s cross sum 23

Setting in	I	II	III	IV	V	yields in	I	II	III	IV	V
0 =	d	l	v	b	s	6 =	j	o	x	r	z
0 =	d	d	d	d		23 =	-	ɱ	b	ɸ	
0 =	l	l	l			23 =	f	ɟ	ʃ		
0 =	v	v				23 =	ɸ	s			
0 =	b					23 =	ɟ				

Groups with the cross sum 29:

j l v b s d o v b s d l x b s d l v r s d l v b z

b l v d s d l s b v

Example 3

Transmitted group q v n y o cross sum 17

Setting in	I	II	III	IV	V	yields in	I	II	III	IV	V
0 =	q	v	n	y	o	12 =	-	-	r	-	-
0 =	q	q	q	q		17 =	ɸ	ɟ	ɱ	ɱ	
0 =	v	v	v			17 =	ʃ	ɸ	ɟ		
0 =	n	n				17 =	b	ɱ			
0 =	y					17 =	ɱ				

Group with the cross sum 29: q v r y o

Doc ID: 6592461

SECTION B

TRANSPOSITION SYSTEMS
Versatzverfahren

In the definition of the production of cryptograms by the transposition system given at the beginning of this study we have already said all that is essential regarding the principle, namely:

1. Preservation of the elements of the plain language,
2. Transposition of the sequence according to definite rules, so that the only question remaining to be discussed is the way in which the plain elements can be transposed among themselves and what security can be attained in this fashion.

1. The limited (short) key number - Die begrenzte Umstellzahl.

One of the simplest methods of transposing the plain elements would consist in reading the plain text in reverse order and thus making it into cipher text. In this case we speak of an Umstellung or shift. This simplest type of shift need not be discussed further because the analysis and solution of the cipher text results automatically.

More usual is the shifting of the plain text with the aid of a limited key number where this shows the sequence in which the elements of the plain text become cipher text. The key number 1 2 3 4 5 6 7 would therefore signify no shift since according to this the plain elements would remain in their original sequence, whereas the key number 7 6 5 4 3 2 1, for instance, would result in breaking up the text into sections of seven elements each and taking the plain text of each section in reverse order as cipher text.

On sheet 1 of Appendix I B 1 a plain text has been enciphered using a random key number. The one-place chain count (digraphic count) on sheet 2, when the cipher elements are arranged according to frequency, not merely shows the plain text frequency curve but is the plain text

Doc ID: 6592461

frequency curve since the sequence of the cipher elements is the same as if a plain text had been subjected to the count.

This result of the count is characteristic of all transposition systems.

A comparison of the parallel passages on sheet 3 of the Appendix shows

1. That the parallel passages occur only at a regular interval of five and
2. That the parallel passages show so-called split off elements (abgesprengte Elemente), i.e. the parallel passages can be expanded forward or backward by single elements within certain short intervals.

These two phenomena, in connection with the plain text frequency of the cipher elements, are characteristic of the limited transposition key with regular repetition. The regular interval between parallel passages reveals the length of the key.

If the transposition segment is marked in the cipher text, it appears that the stray elements before and after the uninterrupted parallel passage do not extend beyond one key segment. Parallels in the plain text, which are separated by an interval not equal to the length of the key, do not appear as parallel passages in the cipher text. Plain parallel passages of slight length which fall in two key segments may also disappear in the cipher text, for instance, the plain "über" in line 2 column 23 and line 6 column 13 of the cipher text no longer attracts our attention as a parallel passage although it is in phase.

Since the detached elements obviously belong to the parallel passage and are merely a result of the transposition, inferences as to the type of transposition may be drawn from their position.

If, taking into account the transposition segments marked in red, a parallel passage like that in row 1, column 6 to 20, reads:

d . e . i	g e i n l	h s . r c*
1 2 3 4 5	1 2 3 4 5	1 2 3 4 5

* Inasmuch as the last two letters of cipher text were incorrectly given here (r c instead of c e) - which error was detected - it is quite possible that other errors exist in parts not checked by the translator.

Doc ID: 6592461

then the last key segment leaves no doubt that in the reconversion to plain text the third cipher element of the key segment must become the fifth plain element of the segment, if the detached elements are to be united with the parallel passage. Furthermore one can conclude from the first key segment by the same line of reasoning that the second and fourth cipher element must become the first and second plain element when re-transposing.

Since according to the first key segment of the parallel passage from line 2 columns 11 to 25

e	.	k	e	r	e	l	u	a	r	.	n	.	g	.
1	2	3	4	5	1	2	3	4	5	1	2	3	4	5

the second cipher element must become the first plain element when retransposed, we can infer from the last segment that the fourth cipher element must become the second plain element.

With this we already know that in retransposing

cipher element	1 2 3 4 5
	↓ ↓ ↓
becomes plain element	. 1 5 2 .

From the first key segment of the parallel passage in line 3 column 16 to 30:

.	.	e	.	d	s	u	h	t	c	n	l	.	a	d
1	2	3	4	5	1	2	3	4	5	1	2	3	4	5

We can infer, after the position of the third cipher element as fifth element has been determined, that the fifth cipher element must become the fourth plain element.

Then the only possibility left for the first cipher element is that it becomes the third plain element so that the entire key reads 3 1 5 2 4. But with this the entire cipher text is solved.

It is also possible, however, to recover the key when the cipher text shows no parallel passages. If German text is involved we can start with the plain digraph ch because plain c virtually never occurs except in combination with h and in rare cases with k.

Doc ID: 6592461

On sheet 4 of the Appendix all the c elements have been listed with the h lying in the vicinity. Just from the h . . c occurring three times in row 1 column 16, row 3 column 6 and row 4 column 11 a regularity may be inferred which suggests transposition. The intervals between these three occurrences are 50 = 2 x 5 x 5, 85 = 5 x 17 and 35 = 5 x 7, which gives the length of the key segment as 5. Since in contrast to the evaluation of parallel passages we here get no clue to the position of c or h in the plain text segment, we can only conclude from the occurrence of h . . . c . / 1 2 3 4 5 / that in the plain text cipher column 4 will stand directly before cipher column 1. In the same way we can conclude from the other occurrences of c and h that cipher column 1 must stand ahead of cipher column 5 and cipher column 5 ahead of cipher column 3, which already permits recovery of the column sequence 4 1 5 3.

Finally it is apparent from the occurrence in row 6 column 21 to 30

/ . . c . . / . h . . / 1 2 3 4 5 1 2 3 4 5 /

that if we are to get the plain text digraph ch, then in retransposing c must move from the third place to the fifth place in the first key segment and h from the second to the first place in the second key segment. Now the sequence of columns can be expanded to 2 4 1 5 3.

As can be seen from the example of encipherment and decipherment at the bottom of sheet 4 of the Appendix, the sequence of plain columns 3 1 5 2 4, which yields the cipher text, corresponds to the sequence of cipher columns 2 4 1 5 3, which converts the cipher text back into the original plain text.

Consequently single digraphs are enough to reach a solution of the entire cipher text. Even though solution calls for more cipher text where the keys are longer, nevertheless the procedure just described is possible as long as the same key number is used repeatedly in succession. Consequently transposition using a limited key number only assures security as long as the ratio between the length of the key and the length of the plain text to be enciphered does not materially exceed about 1 to 3 or 1 to 4.

Doc ID: 6592461

	1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0	
Plain text	l o n d o n x d i e e n g l i s c h e r e g i e r u n g h a	
Shifting	3 1 5 2 4 3 1 5 2 4 3 1 5 2 4 3 1 5 2 4 3 1 5 2 4 3 1 5 2 4	
Cipher text	n l o o d d n e x i g e i n l h s r c e i e r g e g u a n h	1
Plain text	t g e s t e r n e i n e e r k l a e r u n g u e b e r d i e	
Shifting	3 1 5 2 4 3 1 5 2 4 3 1 5 2 4 3 1 5 2 4 3 1 5 2 4 3 1 5 2 4	
Cipher text	e t t g s n e i r e e n k e r c l u a r u n b g e d e e r i	2
Plain text	e n g l i s c h e p o l i t i k i n d e u t s c h l a n d a	
Shifting	3 1 5 2 4 3 1 5 2 4 3 1 5 2 4 3 1 5 2 4 3 1 5 2 4 3 1 5 2 4	
Cipher text	g e i n l h s p c e i o i l t n k e i d s u h t c n l a a d	3
Plain text	b g e g e b e n w e l c h e d i e s e p o l i t i k i n a n	
Shifting	3 1 5 2 4 3 1 5 2 4 3 1 5 2 4 3 1 5 2 4 3 1 5 2 4 3 1 5 2 4	
Cipher text	e b e g g n b e e w h l d e e s i p e e i o i l t n k n i a	4
Plain text	d e r e m l i c h t s e h e n l a e s s t x d i e s e e r k	
Shifting	3 1 5 2 4 3 1 5 2 4 3 1 5 2 4 3 1 5 2 4 3 1 5 2 4 3 1 5 2 4	
Cipher text	r d m e e c l t i h h s n e e e l s a s d t e x i e s k e r	5
Plain text	l a e r u n g s a g t e u e b e r h a u p t n i c h t s i n	
Shifting	3 1 5 2 4 3 1 5 2 4 3 1 5 2 4 3 1 5 2 4 3 1 5 2 4 3 1 5 2 4	
Cipher text	e l u a r s n g g a u t b e e h e u r a n p c t i s h n t i	6
Plain text	b e z u g a u f d e u t s c h l a n d s z u k u n f t x y z	
Shifting	3 1 5 2 4 3 1 5 2 4 3 1 5 2 4 3 1 5 2 4 3 1 5 2 4 3 1 5 2 4	
Cipher text	z b g e u f a c u d s u h t c n l s a d k z n u u x f z t y	7

IB1

1 B 1 - 1

TOP SECRET

Shifting with 5-place key number (U_5) 31524

1-place chain count = digraphic count

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	
a	n_1	r_w	a_3	d_3	r_4	s_5	r_6	u_6	n_6	e_7	d_7																				11
b	g_2	e_4	a_4	e_6	g_7																										5
c	e_1	e_3	n_3	e_4	l_5	t_6	n_7																								7 11
d	d_1	n_1	e_2	s_3	e_3	c_4	m_5	t_5	s_7	k_7																					10 5
e	x_1	i_1	i_1	r_1	g_1	t_2	i_2	e_2	n_2	r_2	l_2	d_2	e_2	r_2	i_3	i_3	i_3	b_4	g_4	e_4	w_4	s_4	e_4	i_4	e_5	c_5	e_5	e_5	l_5	x_5	38 7
f	s_5	r_5	l_6	e_6	h_6	u_6	u_7	u_7																							2 10
g	a_7	z_7																													11
h	e_1	e_{11}	u_1	s_7	e_2	e_3	g_4	n_4	g_6	a_6	e_7																				10 38
i	s_1	e_1	s_3	t_3	l_4	h_5	s_5	e_6	n_6	t_7																					17 2
j	g_1	n_1	e_1	r_2	g_2	m_3	o_3	l_3	d_3	p_4	o_4	l_4	a_4	h_5	e_5	s_6	z_6														- 11
k																															5 10
l	e_2	e_3	n_4	e_5	z_7																										12 17
m	o_1	h_1	w_2	h_3	t_3	a_3	d_4	t_4	t_5	s_5	u_6	s_7																			11 -
n	e_5																														19 5
o	l_1	e_1	l_1	h_1	e_2	k_2	b_2	l_3	k_3	l_3	b_4	k_4	i_4	e_5	g_6	p_6	t_6	l_7	w_7												4 12
p	o_1	d_1	v_3	v_4																											3 11
q	c_3	e_4	c_6																												- 19
r																															10 4
s	c_1	g_1	e_2	e_2	u_2	i_2	d_5	e_5	s_6	a_6																					13 3
t	r_1	n_2	p_3	u_3	v_4	n_5	a_5	d_5	k_5	n_6	h_6	u_7	a_7																		12 -
u	t_2	g_2	n_3	c_3	v_4	i_5	e_5	b_6	i_6	i_6	c_7	y_7																			12 10
v	a_1	a_2	m_2	h_3	a_6	t_6	r_6	f_7	d_7	h_7	u_7	x_7																			- 13
w	h_4																														1 12
x	i_1	i_6	f_7																												3 12
y	$-_7$																														1 -
z	b_7	n_7	t_7																												3 1
																															3
																															1
																															3
																															210

Arrangment of the cipher elements according to their frequency

Cipher elements	e	n	i	s	l	t	u	a	g	d	h	r	c	b	k	o	p	x	z	f	m	w	y
Frequency:	38	19	17	13	12	12	12	11	11	10	10	10	7	5	5	4	3	3	3	1	1	1	1

I b 1 - 2

155

TOP SECRET

Doc ID: 6592461

TOP SECRET

Comparison of parallel passages

Parallel passage	Position	Length	Interval
d · e · i g e i n l h s · c e	1/10. 2/30	8 = 2 · 2 · 2 (+ 4 = 12)	70 = 2 · (5) · 7
e · k e r e l u a r · n · g	2/13. 5/28.	8 = 2 · 2 · 2 (+ 3 = 11)	105 = 3 · (5) · 7
p · e i o i l t n k · i	3/10. 4/20	8 = 2 · 2 · 2 (+ 2 = 10)	40 = 2 · 2 · 2 · (5)
e · d s u h t c n l · a d	3/20. 7/10.	8 = 2 · 2 · 2 (+ 3 = 11)	110 = 2 · (5) · 11
k · e x i	1/8. 5/23	3 = 3 (+ 1 = 4)	135 = 3 · 3 · 3 · (5)

Deductions regarding the numerical shift key for changing plain text into cipher text.

from ←h s ; c e in 1/16-20 · · 5 · ·

from e . k e r→ in 2/11-15 · 1 5 · ·

from d · e · i→ in 1/ 6-10 4 3 1 5 2 3 4

from · · p · e→ in 3/ 6-10 3 1 5 2 4

Final deduction 31524

156

TOP SECRET

Doc ID: 6592461

Doc ID: 6592461

Evaluation of the plain digraph ch:

Position of cipher c and h in the shift section:

		Shift section 1 2 3 4 5	1 2 3 6 5
Line	1/16-20	h · · c ·	
"	3/ 6-10	h · · c ·	
"	3/21-25	· · h · c	
"	4/11-15	h · · c ·	
"	5/ 6-10	c · · · h	
"	6/21-30	· · c · ·	· h · · ·
"	7/11-15	· · h · c	

Deduction regarding the shift key.

4 - 1

4 - 1

5 - 3

4 - 1

1 - 5

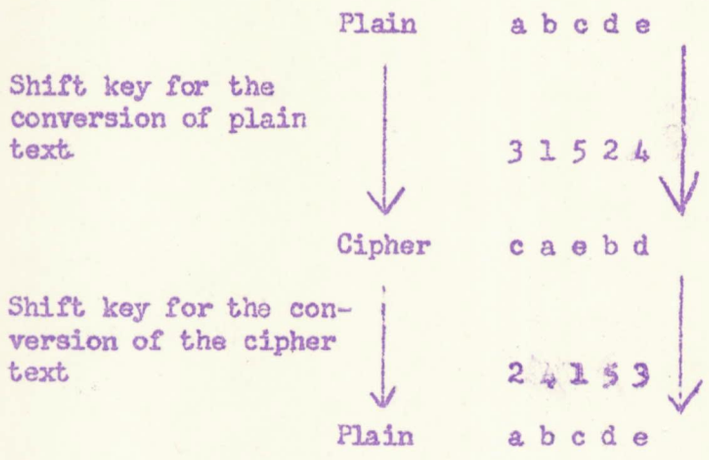
First digit of the shift key = 2, last digit = 3

5 - 3

Final deduction

°4153°
2
24153

Relation of the shift key for the conversion of plain text to the shift key for the conversion of the cipher text.



I B 1 - 4

Doc ID: 6592461

2. Transposition matrix - Der Würfel

More wide spread than the preceding "periodic transposition" involving the use of a short key number (Umstellzahl) is transposition by the aid of a so-called matrix procedure. We speak of a Würfel, or of a columnar transposition of the plain text, as a cryptographic system when the plain text is written out in several rows one beneath the other in a definite width and is taken out column by column according to a key number or with the aid of a key word.

In Appendix I B 2 a the plain text at the top of sheet 1 has been entered below in a box 12 columns wide and 11 rows deep. Above this is the key number. The cipher text is obtained by taking out columns 1,2,3 etc. corresponding to the key and is shown at the bottom of sheet 1.

A count of the cipher text shows no parallel passages. From the occurrence of the individual elements it is clear that a transposition system is involved. Hence it is necessary to see whether inferences can be drawn as to the type of transposition from the position of the single elements of frequent plain digraphs, e.g. the elements c and h.

For this purpose there is a tabulation on sheet 2 showing the positions in the cipher text where these elements are found. For this so-called position count the elements of the cipher text are numbered serially. If the intervals between each two neighboring elements c and h are computed we get for c the intervals

1 2 3 4 5 6 7 9 13 15 15 17 18

and for h the intervals

1 1 1 2 3 4 4 6 7 8 9 11 14 24 27

From this we cannot find any regularity; however the intervals for the two letters show coinciding values for the most part.

If the elements of the cipher text are written out several times one beneath the other on strips and these strips are slid with respect to one another so that two c's always stand beside two h's at the same interval and if the resulting digraphic combinations before, between and

Doc ID: 6592461

after the digraph ch are checked with respect to their probability, then the setting of c in position 28 beside h in position 114 gives below the digraphs gk ei st ch eb he lc sh and above the digraphs di sl ht hn ff gd etc., as shown in the columns number 1 and 2 on sheet 2 of the Appendix. If now against the two h's which are adjacent in column 1 and occupy positions 24 and 25 in the cipher text are set the two c's in positions 66 and 67 using a new strip (see column 3), then the following trigraphs result:

hac hie wgd|iff chn cht ssl rdi ich igk tei ist ich eeb the|hlc lhs etc.

A check shows that between the trigraphs wgd and hlc, which are themselves improbable combinations there stand only quite likely plain text trigraphs, in part very probable trigraphs such as ich, ist, cht.

In like manner the other c's and h's, insofar as they occur at like intervals, can be associated as has been done in columns 7, 6, 5, 4 and 8.

Once trigraphs have been obtained, it is easy by sliding one strip of cipher text to determine where and how an expansion to form syllables and words is possible. Columns 4 and 6, which contain the beginning and end of the cipher text, limit the depth in which a juxtaposition of columns is possible to 11 rows.

With the plain text we then get the exact form of the transposition matrix and the key number with which the cipher text was formed.

This method of solution can also be employed when digraphs like "ch" cannot be juxtaposed, either because they are not found in the plain text or because the h belonging with the c was omitted in encipherment. Although this study may require somewhat more time because the first clues are lacking, it can be made successfully as long as the box has sufficient depth.

The security of the transposition system depends very decidedly on the form of the matrix. This is especially clear in the case of two extreme matrix forms:

Doc ID: 6592461

a) Width 1. The depth corresponds to the length of the message. Plain text and cipher text correspond. There is no cryptogram.

b) Depth 1. The width and the length of the key correspond to the length of the cipher text. There is no possibility of solution unless the key number is used more than once.

From these two extremes it is obvious that a transposition system becomes all the more secure the less the resulting depth of the matrix becomes.

There is no limit to the choice of matrix forms. In Appendix I B 2 b a few other forms are shown which may be used instead of the rectangle, e.g. the comb or the step. However it is also possible to vary the way in which the cipher text is taken out of the matrix, e.g. with the serpentine transposition where the columns are taken out alternately from the top down and from the bottom up or the diagonal transposition where, starting with particular key number values, we take out first the diagonal sequences and then take out the remainder of the elements by columns.

This does not eliminate possibilities of solution because with the step, comb and diagonal transposition some columns always remain undisturbed which can be put together in the familiar manner. Starting with this undisturbed block the irregularities resulting from the deviating matrix forms can be determined very easily. With the serpentine pattern on the other hand the cipher text must be entered on the strips in both directions in order to bring the columns together. Then solution is not more difficult than with the normal pattern.

Doc ID: 6592461

TOP SECRET

Plain text

1 2 3 4 5 6 7 8 9 1̲0 1 2 3 4 5 6 7 8 9 2̲0 1 2 3 4 5 6 7 8 9 3̲0	
d i e s e r b e g r i f f r i c h t e t s i c h n a e m l i	1
c h n i c h t a u s s c h l i e s s l i c h n a c h v e r d	2
i e n s t a u c h n i c h t n a c h f a e h i g k e i t j a	3
n i c h t e i n m a l n a c h h i s t o r i s c h e r w i c	4
h t i g k e i t x	5

Matrix

11 09 05 02 04 10 12 08 01 06 07 03

d	i	e	s	e	r	b	e	g	r	i	f
f	r	i	c	h	t	e	t	s	i	c	h
n	a	e	m	l	i	c	h	n	i	c	h
t	a	u	s	s	c	h	l	i	e	s	s
l	i	c	h	n	a	c	h	v	e	r	d
i	e	n	s	t	a	u	c	h	n	i	c
h	t	n	a	c	h	f	a	e	h	i	g
k	e	i	t	j	a	n	i	c	h	t	e
i	n	m	a	l	n	a	c	h	h	i	s
t	o	r	i	s	c	h	e	r	w	i	c
h	t	i	g	k	e	i	t	x			

Cipher text

1 2 3 4 5 6 7 8 9 1̲0 1 2 3 4 5 6 7 8 9 2̲0 1 2 3 4 5 6 7 8 9 3̲0

g s n i v (h) e (c) (h) r x s (c) m s (h) s a t a i g f (h) (h) s d (c) g e	1
6 9 16 24 25	
s (c) e (h) l s n t (c) j l s k e i e u (c) n n i m r i r i i e e n	2
34	
(h) (h) (h) w i (c) (c) s r i i t i i e t (h) l (h) (c) a i (c) e t i r a a i	3
61 62 63 77 75	
e t e n o t r t i (c) a a (h) a n (c) e d f n t l i (h) k i t (h) b c	4
103 114 118	
(c) (h) (c) u f n a (h) i	5
122 128	

IB2a

TOP SECRET

Doc ID: 6592461

Count of the elements

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	w	x	y	z
9	1	14	2	13	3	3	16	19	1	2	4	2	9	1	-	-	6	9	10	2	1	1	1	- -

Positions of c and h

c: 08 13 28 32 39 48 66 67 80 83 100 106 121 123
5 15 (4) (4) (3) 18 1 13 (3) 17 [6] 15 [2]

h: 06 09 16 24 25 34 61 62 63 77 79 103 114 118 122 128
(3) (7) 8 1 (9) 27 1 1 14 [2] 24 11 (4) (4) [6]

Matching of columns

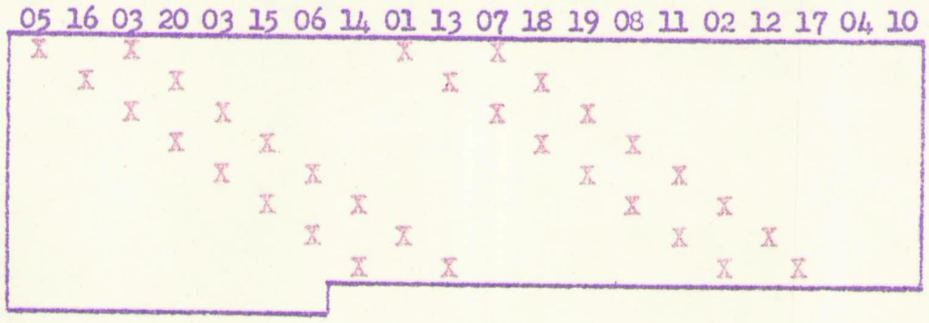
h a c	
h i e	
w : g : d	
i f f	r b e g - r i f f
(c) - h n	t - e - t s i c h n
(c) - h t	i = (c) = h n i c h t
s - s l	c = h l i - e s s l
r d i	a - (c) = h v - e r d i
i - (c) - h	a = u = (c) = h n i c h
i - g k	h f a e h i g k
t - (c) i	a n = i = (c) = h t e i
i - s - t	n - a - (c) = h h i s t
i - (c) - h	c = h - e - r v i c h
e e b	e i t : x : v e e b
t h e	i s (c)
h : l : c	r (c) (c)
l s : (h)	a m s
3 1 2	a s 7 6 5 4 8 (9)

IB 2a - 2

Doc ID: 6592461

Diagonal transposition

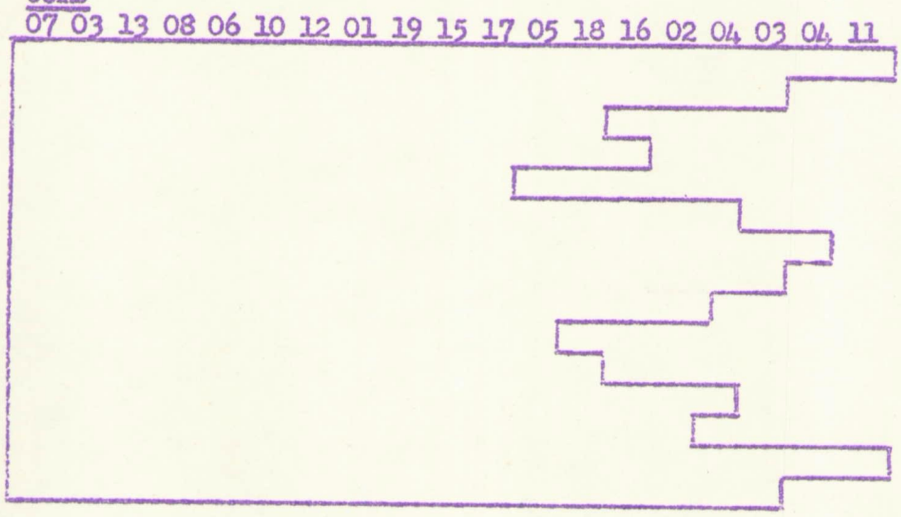
05 16 03 20 03 15 06 14 01 13 07 18 19 08 11 02 12 17 04 10



With 4 diagonals running downward to the right
01, 03, 05, 07

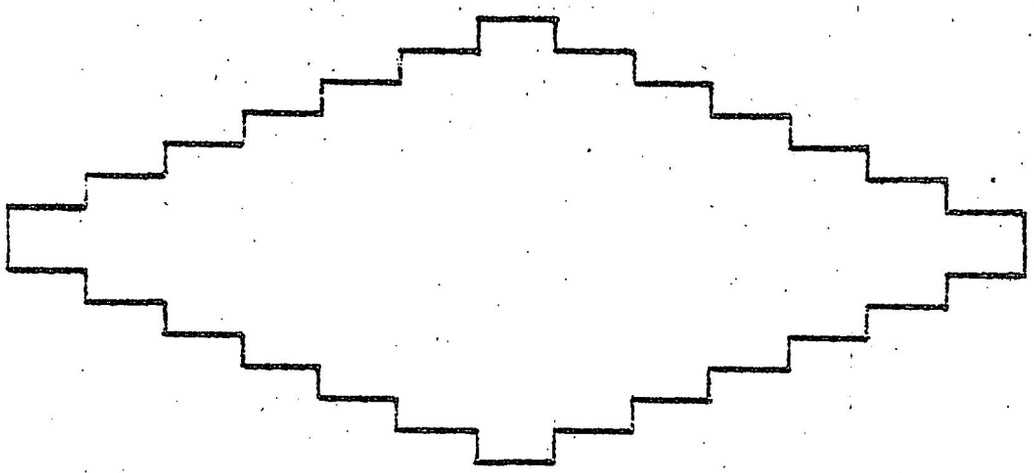
Comb

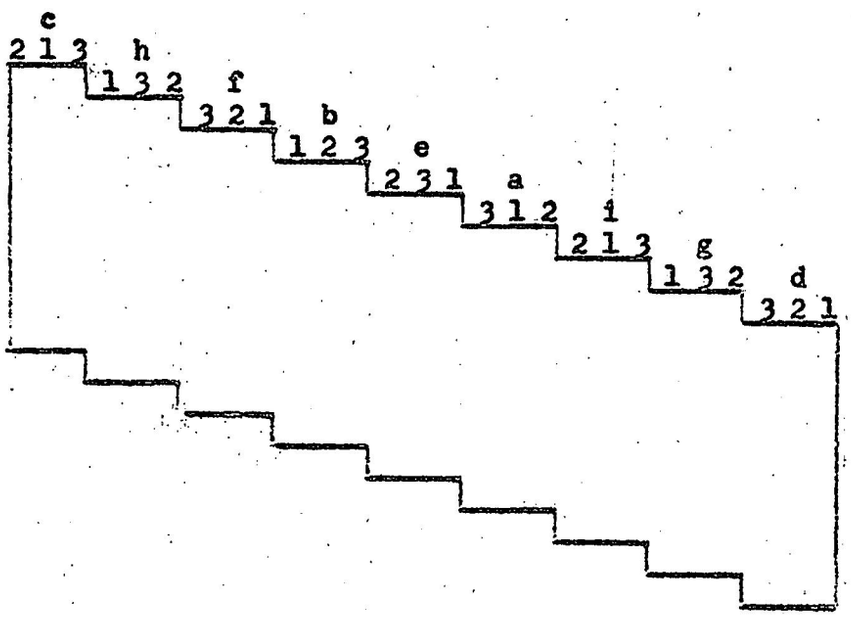
07 03 13 08 06 10 12 01 19 15 17 05 18 16 02 04 03 04 11



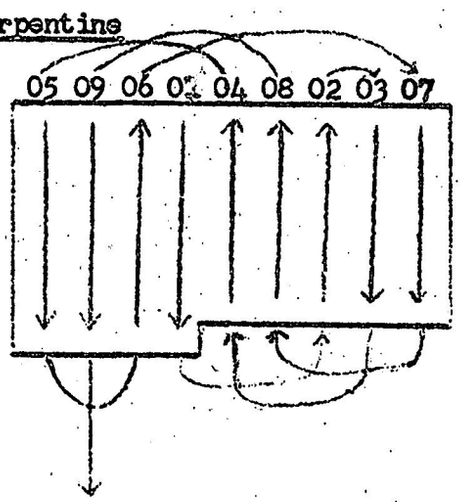
IB26

Stepped





Serpentine



IB 2b - 2

Doc ID: 6592461

3. The grille - Der Raster

Another possibility of transposing the plain elements is afforded by the grille. By a grille we understand a rectangle or square form with several rows and several columns with specific cells punched out by the use of which the cipher text is derived from the plain text. The so-called sliding grille is a rectangular form containing only one punched cell in each column. Otherwise the distribution of the holes is purely optional.

In Appendix I B 3 a the form of a sliding grille is shown on sheet 1 under the plain text. It consists of ten columns and five rows and contains ten grille cells which are distributed over the ten columns at random height.

To encipher the plain text with this sliding grille a rectangle is drawn with a width equal to that of the grille or a width less than that of the grille may be agreed upon; the depth results from the length of the plain text to be enciphered. Then the sliding grille is placed with its bottom row on the top row of this rectangle. In the open cells are inscribed the first elements of the plain text. Then the sliding grille is moved one row down so that its two bottom rows stand on the two top rows of the rectangle. In the open cells is entered the continuation of the plain text. In this way the grille is pushed down a row at a time and used to produce a cipher text. If the grille finally protrudes below the bottom row of the rectangle these lower cells are no longer used for encipherment.

The cipher text at the bottom of sheet 1 of the Appendix was produced in this manner. The 1-place chain count (digraph count) on sheet 2 of the Appendix reveals no parallel passage. From the frequency of the cipher elements it is clear that a transposition is involved. Consequently a position count of the elements c and h is undertaken and this is shown at the bottom of sheet 2. The serial numbering of all cipher elements results in this case from the coordinates of the cipher text on sheet 1.

Doc ID: 6592461

The evaluation of this position count at the bottom of sheet 2 shows, as can be seen from the extract beside it, regular intervals, e.g. for the position values 41, 61, and 161 of c and for the position value 46, 66 and 166 for h, which in turn show regular intervals. On sheet 3 therefore all the elements c and h have been shown in their proper position within the cipher rectangle. The relations between c and h which result have been entered in color.

If the columns are now put together in the sequence and with the degree of displacement indicated by the difference in the position of c to h, e.g. beginning with columns 3 and 7 which stand on the same level, we get plain text such as appears in the juxtaposition of columns at the bottom of sheet 3.

A comparison of the sequence of plain text columns with the original cipher text finally makes possible a reconstruction of the original sliding grille if, beginning with the bottom row, holes are punched in those cells of a grille form containing the first elements of the plain text. A comparison of the beginning of the cipher text at the right on sheet 3 with the grille cells marked in color beneath shows the way this reconstruction is accomplished.

The cipher text obtained with the sliding grille shows a marked relationship with the simple box method. The difference lies in the fact that with the sliding grille the single columns must be juxtaposed at different levels. This displacement of columns, like the sequence of the columns, is a result of the arrangement of the holes in the form. The grille therefore replaces at the same time the key number of the box transposition. Due to the great correspondence of the two systems in their effect on the cipher text both have the same degree of security.

On the other hand the so-called <u>revolving grille</u> has a very different effect on the cipher text. The revolving grille is square and hence has a total of 16 cells if there are four on a side, 25 if there are 5 on a side, 36 if there are 6 on a side, 49 if there are 7 on a side etc. This

revolving grille is turned clock-wise about its center on a cipher square of like size in such fashion that the upper edge of the grille coincides first with the upper edge and then successively with the right edge, bottom edge and left edge of the cipher square. Consequently the punched cells must be so distributed that during a complete revolution each cell of the cipher square becomes visible once. Corresponding to the 4 positions of the revolving grille one quarter of the available cells must be punched out. When the number of cells on a side is odd the central cell remains unused.

In Appendix I B 3 b two revolving grilles with an odd number of cells are shown on sheet 1 and three with an even number of cells on sheet 3. The openings which correspond to one another as the grille is turned are always given the same numerical designation. The punched cells have been shaded in color.

The plain text at the top was enciphered with grille 1 and grille 2 and is contained in the cipher text squares and the cipher text rows 1a and 2a. At the same time there has been enciphered with the two grilles a number sequence from 01 to 25 (see cipher square and cipher text rows 1b and 2b) in order to illustrate the systematic character of the revolving grille.

The encipherment of the number sequence shows that, independent of the form of the revolving grille, certain regularities appear in the transposition resulting from the use of the revolving grille. These regularities are apparent from the schematic representations found on sheet 1 and sheet 3 of the Appendix.

A study of the cipher text shows, in contrast to the preceding transposition systems, a single peculiarity, namely that the length of the cipher text corresponds to the square of a simple number. Hence the length of the message is an important point. If this leads us to infer that a revolving grille has been used, then - due to the effect of each grille opening on four elements, - an assumption as to how two holes are placed with respect to one another always leads to four deductions

regarding the plain text.

Consequently it is a help when solving a revolving grille if one can succeed in picking out in the cipher text plain text digraphs which are characteristic of a language, e.g. ch in German, qu in French, so as to have a fixed starting point.

On sheet 2 of the Appendix is shown the reconstruction of a grille from the cipher text. In row 1a are entered all c's and h's. If it is assumed that the elements c and h taken out of the square to the right form a plain digraph, then two openings have been determined, as shown in the square at the right. From this assumption it also follows that no additional openings can be punched between these two cells. Moreover the fixing of the first two openings rules out the possibility that certain other cells will be openings. All these cells have been crossed out to indicate that they no longer come into account as openings if the original assumption is correct.

From row b it is clear that upon turning the provisional grille once to the right one of the two openings falls on an h. If this h should belong to a digraph ch, only the c in the same row would come into account since due to the peculiarity of the grille the first plain element after the shift remains as the first cipher element. The deductions resulting from this digraph with respect to the opening and to cells not punched are entered once again.

In row c the revolving grille has been returned to its initial position. Since the last hole entered again falls on an h with a c not far ahead of it, the inference is natural that these two elements belong together. After entering the resulting deductions in the revolving grille only four cells remain unmarked.

If, using this provisional grille, the plain text resulting from the four settings is written out in rows d, e, f, and g with a notation of the possible plain text elements for the four questionable cells, then the elements in the upper row can be united with part of those possible in the

lower row to make plain text, if the original assumptions were correct.

The security of the revolving grille is limited by the fact that several messages in the same key can be solved without further ado and that even the security of a single message is not guaranteed. Even though the cipher text offers no clues to characteristic digraphs of the plain text, the regularity inherent in the revolving grille is so great that small grilles at least are always capable of solution.

With larger revolving grilles it is a great disadvantage that the messages have to be padded to fill out the next higher square.

A further disadvantage, which like the time consuming cipher procedure is common to all grilles, is the fact that even minor garbles, in particular the omission of single elements can make the entire message unreadable even for the authorized decrypter.

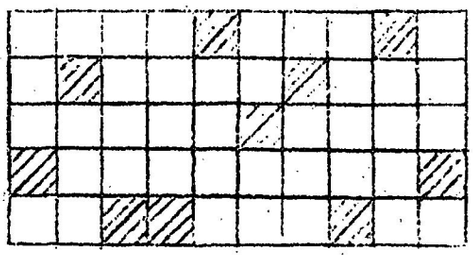
Finally it is a common weakness of all transposition systems that the regularities originating in the plain language lay a transposition system open to attack if it has a systematic structure like the grille and the box. The characteristic thing about the box is that one key number is valid for several rows so that certain depths result.

Of course transposition systems other than the common ones thus far described are conceivable; however this probably will not alter the basic ideas regarding the value and solvability of transposition systems.

Doc ID: 6592461

	0									1									2								
	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9
Plain text	i	c	h	g	l	a	u	b	e	d	a	s	s	e	s	z	i	e	m	l	i	c	h	d	a	s	g	l	e	i
	c	h	e	p	r	o	b	l	e	m	i	n	a	l	l	e	n	w	i	s	s	e	n	s	c	h	a	f	t	e
	n	i	s	t	x	a	b	s	i	c	h	t	l	i	c	h	h	a	b	e	i	c	h	v	e	r	m	i	e	d
	e	n	d	i	e	v	e	r	s	c	h	i	e	d	e	n	e	n	r	i	c	h	t	u	n	g	e	n	z	u
	b	e	s	p	r	e	c	h	e	n	x	e	s	i	s	t	z	e	i	t	e	n	d	l	i	c	h	s	c	h
	l	u	s	s	z	u	m	a	c	h	e	n	m	i	t	u	n	t	e	r	s	c	h	i	e	d	e	n	x	y

Grille — Shaded cells represent openings



Cipher text

	0	1	2	3	4	5	6	7	8	9
0	g	s	i	c	h	e	z	h	d	l
1	d	a	a	u	e	i	s	b	p	a
2	e	r	s	s	a	g	o	e	l	m
3	l	l	l	i	n	b	e	c	s	e
4	l	c	i	c	s	n	h	h	t	e
5	v	x	m	i	l	a	a	n	i	i
6	f	c	s	s	h	b	h	e	v	t
7	s	e	e	n	d	h	r	i	i	i
8	a	e	c	h	e	m	v	t	d	b
9	i	e	e	i	t	e	n	c	u	e
10	r	n	d	c	s	e	g	n	p	s
11	n	r	c	h	s	e	e	i	i	r
12	n	s	i	c	d	c	t	h	l	z
13	h	i	u	b	s	z	c	e	s	e
14	e	z	n	x	m	h	u	e	i	i
15	s	t	t	e	r	m	u	n	s	c
16	a	c	h	l	e	n	h	u	d	c
17	t	e	h	e	x	i	n	n	y	e

The grille is placed with its bottom row on the top row of the rectangle whose width corresponds to that of the grille and whose depth corresponds to the length of the text and the plain text is entered in the open cells. Then the grille is moved downward a row at a time and the plain text entered in the open cells.

I b 3 a - 1

IB3a

Doc ID: 6592461

TOP SECRET

1-place chain count - digraphic count

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	
a	a_1	u_1	e_1	g_2	a_5	n_5	e_8	c_{16}													8
b	p_1	e_3	h_6	i_8	s_{13}																5
c	h_0	s_3	i_4	s_4	s_6	h_8	u_5	h_{11}	d_{12}	t_{12}	e_{13}	a_{15}	h_{16}	t_{16}							14
d	l_0	a_1	h_2	b_8	e_{10}	c_{12}	c_{16}														7
e	z_0	i_1	r_2	l_2	c_2	l_3	w_4	v_6	e_7	n_7	c_8	m_8	e_9	i_3	n_3	r_3	s_{10}	g_{10}	e_{11}	i_{11}	28
f	e_{13}	e_{13}	z_{14}	n_{15}	n_{16}	h_{17}	x_{17}	y_{17}													1
g	c_6																				3
h	s_0	o_2	n_{10}																		15
i	e_0	d_0	h_4	t_4	b_6	e_6	r_2	e_8	s_{11}	l_{12}	i_{13}	u_4	l_{16}	u_{16}	e_{17}						20
j	o_0	s_1	n_3	c_4	l_5	i_5	f_5	i_7	i_7	a_7	k_3	t_3	i_{11}	r_{11}	c_{12}	u_{13}	i_{14}	i_{14}	s_{14}	n_{17}	-
k																					-
l	d_0	m_2	l_3	l_3	i_3	q_4	a_5	z_{12}	e_{16}												9
m	l_2	i_5	v_8	h_{14}	u_{15}																5
n	b_3	d_4	i_5	d_7	c_3	d_{10}	p_{10}	r_{10}	s_{12}	x_{14}	s_{15}	h_{16}	n_{17}	y_{17}							14
o	e_2																				1
p	a_1	s_{10}																			2
q																					-
r	s_2	i_7	n_{10}	q_{10}	x_{11}	m_5															6
s	i_0	b_1	s_2	a_2	e_3	n_4	s_6	h_6	e_7	e_{10}	n_{10}	e_{11}	i_{12}	z_{13}	e_{13}	t_{15}	q_{15}				17
t	q_4	s_6	d_8	e_9	h_{12}	t_{15}	e_{15}	e_{17}													8
u	e_1	e_8	b_{13}	e_{14}	n_{15}	d_{16}															6
v	t_6	t_8																			2
w	x_5																				1
x	m_5	m_{14}	i_{17}																		3
y	e_{16}																				1
z	h_0	h_{12}	c_{13}	n_{14}																	4

180 elements

Elements arranged according to frequency.

Elements	e	i	s	h	c	n	l	a	t	d	r	u	b	m	z	g	x	p	v	f	o	w	y	j	k	q
Frequency	28	20	17	15	14	14	9	8	8	7	6	6	5	5	4	3	3	2	2	1	1	1	1	-	-	-

Positions of the elements c and h

c = 03 37 41 43 61 82 97 112 123 125 136 153 161 169

h = 04 07 46 47 64 66 75 83 11- 127 130 145 162 166 172

41 ← 5 → 46
↕ 20 ↕ 20
61 ← 5 → 66
↕ 100 ↕ 100
161 ← 5 → 166

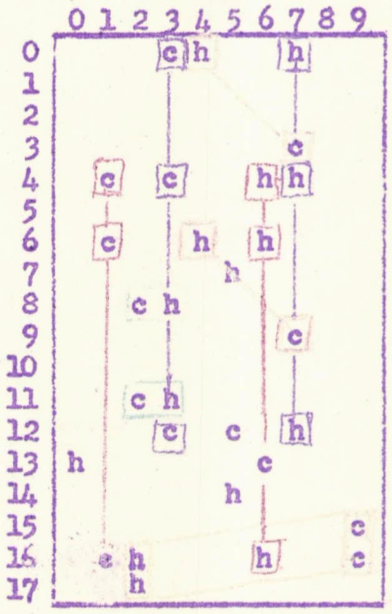
TOP SECRET

Doc ID: 6592461

TOP SECRET

Position of the elements

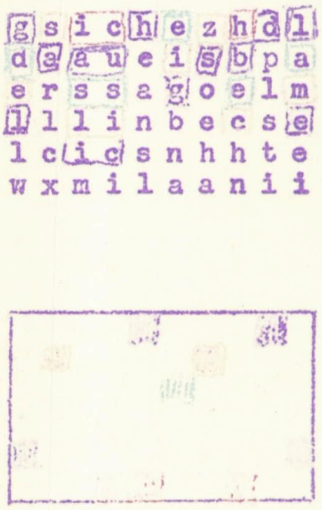
"c" and "h" in the cipher text



Composition of the columns

Sequence of the columns 0 9 2 3 7 4 8 1 6 5

0 1 2 3 4 5 6 7 8 9



IB 3 a - 3

TOP SECRET

Doc ID: 6592461

TOP SECRET

1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5

Plain text: u n r e c h t g u t g e d e i h t s c h l e c h t

Grille

1)

1	2	3	4	1
4	5	6	5	2
3	6	(7)	6	3
2	5	6	5	4
1	4	3	2	1

2)

1	2	3	4	1
4	5	6	5	2
3	6	(7)	6	3
2	5	6	5	4
1	4	3	2	1

Cipher text

1a)

c	t	u	g	n
r	d	u	h	e
l	e	t	i	t
c	g	e	h	h
t	c	s	h	e

1b)

19	07	01	08	02		
03	13	09	20	14		
21	04	25	15	10		
05	11	22	06	16		
17	23	18	24	12		

2a)

d	c	t	e	h
g	u	i	u	n
r	t	t	l	h
t	e	e	s	c
g	c	h	c	h

2b)

13	19	07	14	20		
08	01	15	09	02		
03	10	25	21	16		
17	22	04	18	23		
11	05	24	12	06		

1a: c t u g n r d u h e l e t i t c g e h h t c s h e

1b: 19 07 01 08 02 03 13 09 20 14 21 04 25 15 10 05 11 22 06 16 17 23 18 24 12

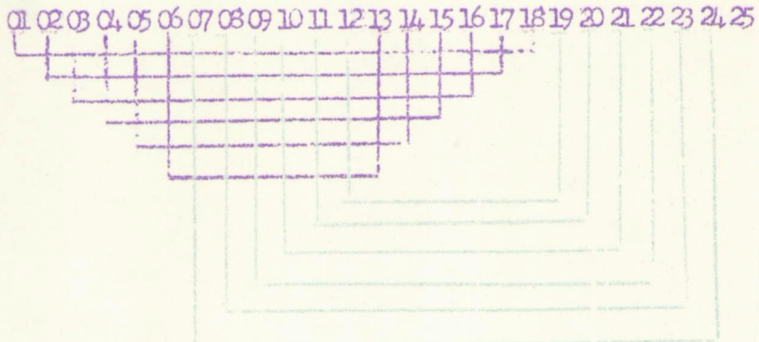
2a: d c t e h g u i u m r t t l h t e e s c g c h e h

2b: 13 19 07 14 20 08 07 05 09 02 03 10 25 21 16 17 22 04 18 23 11 05 24 12 06

Regularity in the formation of digraphs

u n r e c h t g u t g e d e i h t s c h l e c h t

01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25



IB 3 b - 1

IB3b

TOP SECRET

Doc ID: 6592461

TOP SECRET

Reconstruction of the grille

= open cell = no opening possible

1a)

c	t	u	g	n
r	d	u	h	e
l	e	t	i	t
c	g	e	h	h
t	c	s	h	e

b)

c) d) e) f) g)

c h . . . c h t
l e t e (25)
(.)

. n r . . c h .
u u e s

t g . . . . g e
u l i t

. d e . . h t
u i e s

TOP SECRET

Grille

1	2	3	7	4	1
4	5	6	8	5	2
7	8	9	9	6	3
3	6	9	9	8	7
2	5	8	6	5	4
1	4	7	3	2	1

1	2	3	7	[illegible]	1
4	5	6	8	5	2
7	8	[illegible]	9	[illegible]	3
[illegible]	6	9	9	8	[illegible]
2	5	8	6	5	4
[illegible]	4	7	3	[illegible]	1

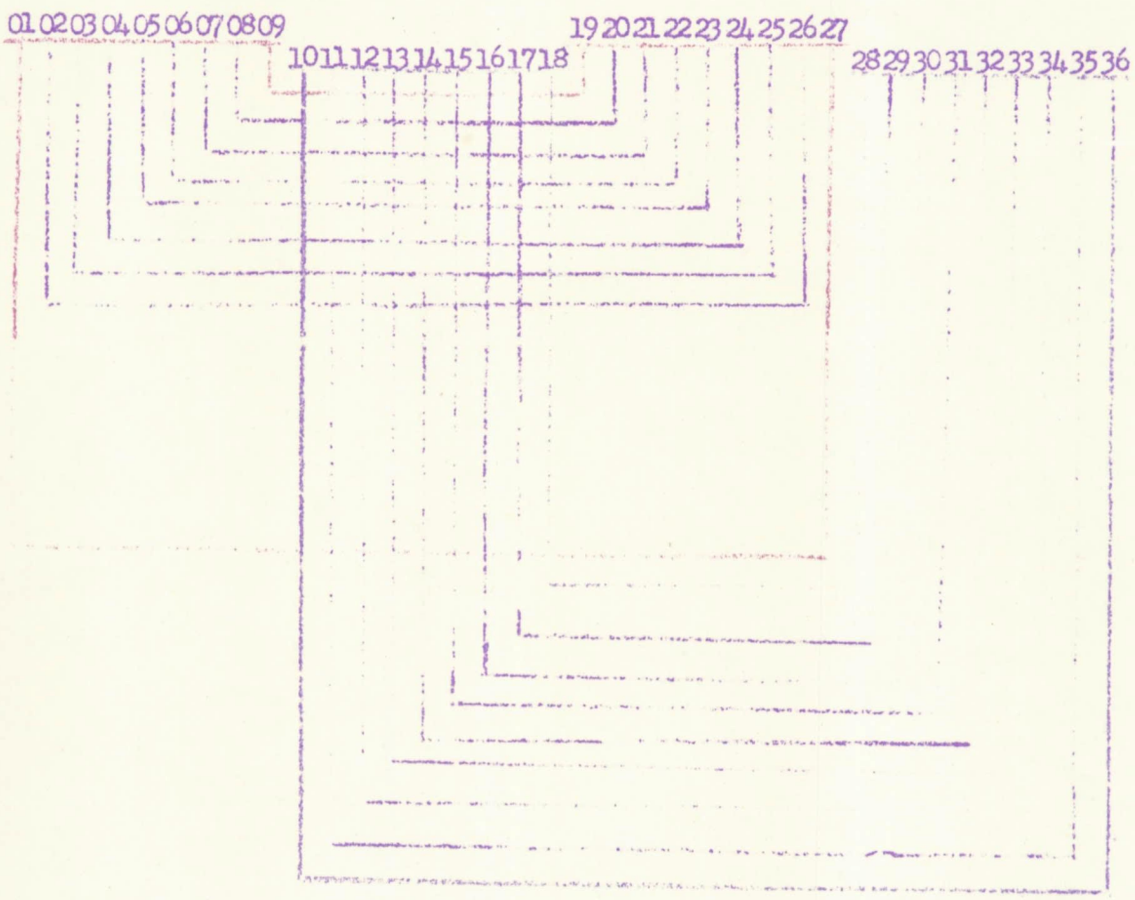
Plain text 01 02 03 04 . . . . . 34 35 36

Cipher text

10	01	28	02	29	19
20	11	21	12	22	13
30	03	31	04	32	05
23	14	24	15	26	16
33	06	34	07	35	08
09	17	26	18	27	36

10	19	11	28	01	20
29	02	30	21	12	31
22	13	03	14	04	23
05	24	32	25	33	06
15	34	07	16	26	17
08	27	18	35	09	36

Regularity of digraphs



IB 3b - 3

Doc ID: 6592460

ARMED FORCES SECURITY AGENCY

DF-240 Part II

5/52/~~TOPSEC~~/AFSA-14

Copy No. 35

From: AFSA-14

To: ARCHIVES, AFSA 252 H

/THIS DOCUMENT CONTAINS INFORMATION AFFECTING THE NATIONAL DEFENSE OF THE UNITED STATES WITHIN THE MEANING OF THE ESPIONAGE LAWS, TITLE 18, U.S.C., SECTIONS 793 and 794. SEE ALSO PUBLIC LAW 513, 81ST CONGRESS, SECOND SESSION. ITS TRANSMISSION OR THE REVELATION OF ITS CONTENTS IN ANY MANNER TO AN UNAUTHORIZED PERSON IS PROHIBITED BY LAW./

Approved for Release by NSA on 09-12-2017, FOIA Case #67677

Doc ID: 6592460

DF-240 Part II 5/52/~~TOPSEC~~/AFSA-14

CHARACTERISTICS, ANALYSIS AND SECURITY OF CRYPTOGRAPHIC SYSTEMS

1. Attached is an Armed Forces Security Agency translation of Part II of a treatise on cryptology prepared by Dr. Bruno KRÖGER, formerly with the Forschungsamt. German title: Systematik, Analyse und Sicherheit der Geheimschriften.

2. This treatise purports to cover in detail the work given in the course at the Forschungsamt. Since the methods described here are NOT essentially different from those used by AFSA, the primary value will be found in the picture it gives of the approach to these problems of another major cryptologic unit.

3. Appendices follow the section of text which they illustrate.

Translated: R.W.P. 35 copies
January 1952
Distribution: Normal 57 pages

Request to all holders of DF-240 Part II:

Kindly change the second sentence of the second paragraph on page 2 to read:

"Since the methods described here are NOT essentially ..... "

THANK YOU

TABLE OF CONTENTS

		Page
II.	Combined and superenciphered systems	5
A.	Combined systems	5
	Kombinierte Verfahren	
1.	Double transposition	6
	Der Doppelwürfel	
	a) Messages of the same length in the same key	
	Schlüsselgl. Sprüche gleicher Länge	
	b) Messages of similar length in the same key	
	Schlüsselgl. Sprüche ähnlicher Länge	
2.	Matrix transposition with grille	19
	Würfel mit Raster	
3.	Substitution with short transposition key	26
	Cäsar mit Umstellzahl	
4.	Substitution with matrix transposition	27
	Cäsar mit Würfel	
5.	Code with short transposition key	28
	Code mit Umstellzahl	
6.	Code with matrix transposition	29
	Code mit Würfel	
7.	Polyalphabetic substitution with short transposition key or with matrix	30
	Spaltencäsaren mit Umstellzahl oder Würfel	
B.	Superenciphered systems	31
	Überschlüsselte Verfahren	
1.	Encipherment by substitution table	31
	Tauschtafelüberschlüsselungen	
	a) One-place substitution tables	
	Einstellige Tauschtafeln	
	b) Multi-place substitution tables	
	Mehrstellige Tauschtafeln	

Doc ID: 6592460

TOP SECRET

Page

2. Additive 35

Die Überschlüsselungszahl

a) Addition modulo 10

Symbolische Addition

b) Differencing method

Differenzenmethode

c) Difference catalogue

Differenzenkatalog

d) Additive tables

Überschlusselungszahlentafeln

e) Generation from key numbers

Entwicklung aus Schlüsselzahlen

3. Additive sequence for codes with groups of varying length 53

Überschlüsselungszahlen für wechselstellige Codes

4. Additive in the substitution table system 54

Überschlüsselungszahlen im Tauschtafelverfahren

TOP SECRET

COMBINED AND SUPERENCIPHERED SYSTEMS

Since to a great extent the basic systems have not met security requirements, there has been an ever increasing tendency to encipher once again the text already enciphered in the basic system in order in this way to achieve a higher degree of security.

When one of the known basic systems is used for the second encipherment, we have a combination of two basic systems and speak of combined systems in contrast to the superenciphered systems where special methods have been developed for treating the cipher text produced by a basic system.

SECTION A

COMBINED SYSTEMS
(Kombinierte Verfahren)

The extent to which increased security of a cryptogram can be achieved by reenciphering a text produced by a basic system making use of a second basic system depends upon the choice of the basic systems to be combined. For instance a second encipherment of a single substitution text using a second substitution alphabet yields no increase in security because the unauthorized decrypter would not notice that there had been an intermediate encipherment. If in the first alphabet a = b and in the second substitution b = c, it would be simplier to substitute at the outset a = c and the security would be the same.

1. Double transposition

(Der Doppelwürfel)

On the other hand if a cipher text enciphered by a matrix transposition is reenciphered with a second matrix, the result is quite different. After the first encipherment it is still possible by writing out the cipher text on strips and by sliding the strips to determine the positions in which fragments of plain text are formed at a certain depth; the same course of solution is no longer of use when the first cipher text has been reenciphered by transposition, i.e. when we have a double transposition as it is called. When following the same method of solution used for single transposition, the problem would be to find by sliding these strips those positions in which the cipher text of the first matrix arises. Since the criteria available for a plain text cannot be applied in the case of a cipher text, this problem is incapable of solution.

The unauthorized decrypter confronted with a single text produced by double transposition is usually merely able to determine that a transposition system is involved. All attempts at solution with a single text are doomed to failure unless it be that the plain text contains exceptionally long parallel passages.

Even when one and the same double transposition is used a number of times for different texts there is usually no possibility for the unauthorized decrypter to break into the system as long as the texts are of distinctly different lengths and contain no relatively long parallel passages.

Only in special cases where several cipher texts of identical length and in the same key are available, where the cipher text shows exceptionally long parallel passages which must extend at least over two box widths of the first word, or where the same double transposition was used for several messages of approximately equal length and these messages contain rather long parallel passages which exceed the width of the first matrix, is it possible to solve the double transposition from the cipher text.

In Appendix II A 1 a on sheet 1 is a text of 180 elements divided into six sections I to VI of 30 elements each. Beneath are the two matrices with keys by which these sections are enciphered. In matrix I the first thirty elements are represented by the numbers 01 02 03 ... 30. Matrix II contains the cipher text produced by the first transposition 03 08 13 18 23 etc. From this matrix II is derived the cipher text II corresponding to the key. At the bottom of sheet 1 are the 6 cipher texts with designation of the plain columns (or of the shift number (Umstellzahl) produced by the double transposition).

A solution is sought by first arranging the cipher text columns (e.g. on the basis of like indicator groups and like length) so that plain text results. In the German language the plain digraph ch or ck may afford a starting point. After marking the elements c, h and k in the cipher text it is obvious that columns 12 and 13 belong together. From the c and h remaining in cipher text V it is apparent that columns 28 and 29 belong together.

These pairs of columns 12 13 and 28 29 are written out at the top of sheet 2. A check of the resulting plain digraphs shows that the 2nd, 3rd, 4th, 5th and 6th digraph of columns 28 and 29 probably call for a preceding vowel in German. Only column 27 contains five vowels in the 2nd to 6th position. The 1st, 3rd, and 5th digraphs of columns 12 and 13 likewise call for a preceding vowel. Only columns 11 and 24 come into account. Starting with the trigraphs thus obtained it is easy to match the remaining columns.

By comparing the plain text thus obtained with the cipher text it is possible to obtain the numerical key.

Since this key has been derived in systematic fashion from the double transposition, it is a question of recognizing the systematic feature by studying the sequence of cipher columns. For this purpose the difference between the column designations, of which the key number is composed, have

been derived at the bottom of sheet 2. These differences reveal parallel passages. If the sequence of cipher columns is divided up in differences corresponding to these parallel passages and if these segments are then arranged by columns corresponding to their first digits, the result is the arrangement shown lower down on the sheet which reveals the systematic character of matrix II. After that it is an easy matter to derive matrix I from matrix II as shown at the bottom of sheet 2.

On sheet 3 is given a second example of the reconstruction of the transposition matrices. Although the parallel passages in the differences are not quite so clear here because of the wider but shallower matrices, we do get the division into columns for the entire sequence of columns. The first elements of these columns can be arranged by the interval 7 (i.e. the width of the first matrix) into the series 01 08 15 and 05 12 19 26 33, which together yield the first row of matrix II. If we enter first the complete row 05 12 19 26 33 and then the row beginning 01 08 15 (which is supplemented by 22 29 in the second row of the matrix), the reconstruction of matrix I follows as a matter of course.

This proves that several messages in the same key will lead to the reconstruction of the two matrices if the messages have the same length.

When messages in the same key reveal parallel passages extending beyond one row of the first matrix, then solution is possible if the messages are of approximately the same length.

An example has been worked out in Appendix II A 1 b. The three plain texts of the example have 58, 56 and 90 elements respectively and have the same plain text beginning (something which occurs all too often in actual traffic because of stereotyped references and telegram beginnings). These three texts have been enciphered on sheet 1 with the same double transposition and the parallel passage has been underscored in red. A check of the columns of matrix II for plain texts A B and C which yield the cipher

text, reveals that texts A and B with the similar lengths of 58 and 56 elements still contain recognizable fragments of the original parallel passages, while the fragments in the longer text of 90 elements are so distributed that the passage can no longer be recognized in the cipher text.

At the top of sheet 2 cipher texts A and B have been written out. Underneath is a 1-place chain count made to discover the parallel passages. These parallel passages, which consist merely of digraphs, have been marked in color in the cipher text and have been framed in red insofar as their position in the cipher texts is identical or corresponds to the difference in length.

From the distribution of the like or almost like positioned parallel passages in text A and B we infer there are six columns and therefore that the width of matrix II is 6. From this and from the length of the messages we get for cipher text A a matrix II with four columns of ten elements and two columns of nine elements and for cipher text B a matri x with two columns of ten elementsand four columns of nine elements.

If the like positioned digraph [er] in the first row of text A and B is not to be torn apart, we get for column 1 of text A and B a depth of 9 elements. The division into columns has been indicated in the cipher text by ↕ . It is now possible to indicate by one or more vertical lines || the possible positions for separating the other columns, taking into consideration the number with the depth of 9 and with the depth of 10.

From the possible separation

in cipher text A: . . . . s f | i | t i z . . . . . and

in cipher text B: . . . . r u | e | i z . . . . . .

it results that only the separation between i and t in text A and between u and e in text B, i.e.

in cipher text A: . . . . s f i ↕ t i z . . . . .

in cipher text B: . . . . . r u ↕ e i z . . . . .

can convert the almost like positioned digraph iz into a like positioned one in the matrix. With this the depth of column 2 in text A is fixed at 10 and in text B at 9 elements.

In corresponding fashion the almost like positioned digraph se can be made a like positioned digraph if the separation for column 6 (↕) is made between e and s in cipher texts A and B.

With this the length of columns 1, 2 and 6 are determined. Once the length of these columns is fixed their possible position in matrix II is limited. Under 1) on sheet 3 are shown the possible positions of columns 1, 2 and 6 in the matrix.

Now if the repeated digraphs which are not in like position and which stand in different columns in text A and B are not accidental, then from their position we can deduce in connection with the message lengths of 58 and 56 elements that the B-column in which a repeated digraph appears must stand ahead of that A-column in which this digraph appears again. Moreover these columns must stand at an interval of 1 or of 2 because the total length of messages A and B differs by only two elements.

Under 2) on sheet 3 these repeated digraphs are shown with their positions and the resulting inferences regarding the sequence of columns is noted at the right.

Since it was shown under 1) that column 2 and column 6 can stand only in the 3rd or 4th position in the matrix and since it is shown under 2) that

columns 2 and 6 follow one another at an interval of one or two, it is certain that column 2 must stand in the 3rd position and column 6 in the 4th position in matrix II.

If column 3 or 5 is to stand ahead of column 6 at an interval of 1 or 2, it results that only the second column of the matrix remains open. This enables us to place column 4 in the first position.

Since it may also be assumed that the like positioned digraphs ad in columns A1 and B1 and iz in columns A3 and B3 are adjacent in both matrices, we deduce from that as shown under 4) on sheet 2, that columns 1 and 3 are adjacent and therefore occupy the 5th and 6th positions in the matrix.

With this the key number or the column sequence of Box II is fixed either as 4 5 2 6 1 3 or as 4 5 2 6 3 1. When the columns from sheet 2 are put together in these sequences on sheet 4, the parallel passages show that the sequence 4 5 2 6 1 3 is the correct one.

The parallel passages in matrix II designate at the same time the beginning and end of the columns from matrix I as written out on sheet 4 at the bottom. The matching of these columns to get plain text, i.e. the reconstruction of matrix I, causes less difficulty since it results from the length of columns under A that the 3rd and 5th columns must stand in the 1st or 2nd position in matrix I.

The combination of two matrices for a double transposition has therefore brought a significant increase in security because a single text enciphered by double transposition is not capable of solution and even where several messages in the same key are available a solution is possible only under very definite conditions.

TOP SECRET

		1	2	3	4	5	6	7	8	9	1 0	1	2	3	4	5	6	7	8	9	2 0	1	2	3	4	5	6	7	8	9	3 0
Plain text	I	k	u	e	n	s	t	l	e	r	d	i	c	h	t	e	r	u	n	d	p	h	i	l	o	s	o	p	h	e	n
	II	h	a	b	e	n	z	w	e	i	e	r	l	e	i	f	u	n	k	t	i	o	n	x	d	e	n	i	n	n	e
	III	r	e	n	g	e	h	a	l	t	d	e	r	z	e	i	t	u	n	d	w	e	l	t	i	d	e	a	l	z	u
	IV	r	a	n	s	c	h	a	u	u	n	g	z	u	b	r	i	n	g	e	n	u	n	d	i	h	n	a	l	s	u
	V	n	v	e	r	g	a	e	n	g	l	i	c	h	e	k	u	n	d	e	a	u	f	d	i	e	n	a	c	h	w
	VI	e	l	t	z	u	u	e	b	e	r	l	i	e	f	e	r	n	x	j	x	b	u	r	c	k	h	a	r	d	t

Box I

2	4	1	3	5
01	02	03	04	05
06	07	08	09	10
11	12	13	14	15
16	17	18	19	20
21	22	23	24	25
26	27	28	29	30

Box II

4	1	3	2
03	08	13	18
23	28	01	06
11	16	21	26
04	09	14	19
24	29	02	07
12	17	22	27
05	10	15	20
25	30		

Cipher text I 03 08 13 18 23 28 01 06 11 16 21 26 04 09 14 19 24 29 02 07 12 17
22 27 05 10 15 20 25 30

Cipher text II 08 28 16 09 29 17 10 30 18 06 26 19 07 27 20 13 01 21 14 02 22 15
03 23 11 04 24 12 05 25

		08	28	16	09	29	17	10	30	18	06	26	19	07	27	20	13	01	21	14	02	22	15	03	23	11	04	24	12	05	25
Cipher text		I	e	h	r	r	e	u	d	n	n	t	o	d	l	p	p	h	k	h	t	u	i	e	e	l	i	n	o	c	s	s
"	"	II	e	n	u	i	n	n	e	e	k	z	n	t	w	i	i	e	h	o	i	a	n	f	b	x	r	e	d	l	n	e
"	"	III	l	l	t	t	z	u	d	u	n	h	e	d	a	a	w	z	r	e	e	e	l	i	n	t	e	g	i	r	e	d
"	"	IV	u	l	i	u	s	n	n	u	g	h	n	e	a	a	n	u	r	u	b	a	n	r	n	d	g	s	i	z	c	h
"	"	V	n	c	u	g	h	n	l	w	d	a	n	e	e	a	a	h	n	u	e	v	f	k	e	d	i	r	i	c	g	e
"	"	VI	b	r	r	e	d	n	r	t	x	u	h	j	e	a	x	e	e	b	f	l	u	e	t	r	l	z	c	i	u	k

II A 1 a - 1

TOP SECRET

Doc ID: 6592460

TOP SECRET

Matching cipher columns

	12	13
(v)	c	h
	l	e
(v)	r	z
	z	u
v	c	h
	i	e

either

11	12	13
i	c	h
r	l	e
e	r	z
g	z	u
i	c	h
l	i	e

or

11	12	13
o	c	h
d	l	e
i	r	z
i	z	u
i	c	h
c	i	e

27		28	29		30
p	-	h	e	=	n
i	v	n	n	=	e
a	v	l	z	=	u
a	v	l	s	=	u
a	v	c	h	=	w
a	v	r	d	=	t

Sequence of cipher columns with differences

Sequence of cipher columns: 08 28 16 09 29 17 10 30 18 06 26 19 07 27 20

Differences: 20 18 23 20 18 23 20 18 18 20 23 18 20 23 23

II IV

Sequence of cipher columns: 13 01 21 14 02 22 15 03 23 11 04 24 12 05 25

18 20 23 18 20 23 18 20 18 23 20 18 23 20

III I

I II III IV

4	1	3	2
03	08	13	18
23	28	01	06
11	16	21	26
04	09	14	19
24	29	02	07
12	17	22	27
05	10	15	20
25	30		

→

03	08	13	18	23	28
01	06	11	16	21	26
04	09	14	19	24	29
02	07	12	17	22	27
05	10	15	20	25	30

→

2	4	1	3	5
01	02	03	04	05
06	07	08	09	10
11	12	13	14	15
16	17	18	19	20
21	22	23	24	25
26	27	28	29	30

TOP SECRET

Doc ID: 6592460

II
Ala3

Example of the reconstruction of the two boxes

Plain text: 01 02 03 04 05 06 33

Box I

2	7	5	7	1	4	3
2	7	5	6	1	4	3
01	02	03	04	05	06	07
08	09	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31	32	33		

Box II

3	6	1	8	5	2	7	4
05	12	19	26	33	01	08	15
22	29	07	14	21	28	06	13
20	27	03	10	17	24	31	04
11	18	25	32	02	09	16	23
30							

Cipher text

Sequence of columns	19	07	03	25	01	28	24	09	05	22	20	11	30	15	13	04
Differences	21	29	22	09	27	29	18	29	17	31	24	19	18	31	24	19

Sequence of columns	23	33	21	17	02	12	29	27	18	08	06	31	16	26	14	10	32
Differences	10	21	29	18	10	17	31	24	23	31	25	18	10	21	29	22	

The elements of the first row of Box II: 19 01 05 15 33 12 08 26

01 08 15

05 12 13 26 33

Hence Box II reads:

3	6	1	8	5	2	7	4
05	12	19	26	33	01	08	15
22	29	07	14	21	28	06	13
20	27	03	10	17	24	31	04
11	18	25	32	02	09	16	23
30							

and Box I reads:

2	7	5	6	1	4	3
01	02	03	04	05	06	07
08	09	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31	32	33		

Doc ID: 6592460

TOP SECRET

II Albl

		1								2								3		
		1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0
Plain text	A	d	e	r	f	r	a	n	z	o	e	s	i	s	c	h	e	a	u	s	s
e	n	m	i	n	i	s	t	e	r												
		e	m	p	f	i	n	g	g	e	s	t	e	r	n	e	i	n	e	d	e
l	e	g	a	t	i	o	n														58
	B	d	e	r	f	r	a	n	z	o	e	s	i	s	c	h	e	a	u	s	s
e	n	m	i	n	i	s	t	e	r												56
		s	p	r	a	c	h	v	o	r	d	e	r	a	u	s	l	a	n	d	s
p	r	e	s	s	e																
	C	d	e	r	f	r	a	n	z	o	e	s	i	s	c	h	e	a	u	s	s
e	n	m	i	n	i	s	t	e	r												
		e	r	k	l	a	e	r	t	e	v	o	r	d	e	m	r	a	t	d	e
r	r	e	p	u	b	l	i	k	d												
		a	s	n	e	u	e	a	b	k	o	m	m	e	n	m	i	t	d	e	m
s	a	e	r	g	e	b	i	e	t												90

Box I

A

3	5	2	7	6	1	4
d	e	r	f	r	a	n
z	o	e	s	i	s	c
h	e	a	u	s	s	e
n	m	i	n	i	s	t
e	r	e	m	p	f	i
n	g	g	e	s	t	e
r	n	e	i	n	e	d
e	l	e	g	a	t	i
o	n					

B

3	5	2	7	6	1	4
d	e	r	f	r	a	n
z	o	e	s	i	s	c
h	e	a	u	s	s	e
n	m	i	n	i	s	t
e	r	s	p	r	a	c
h	v	o	r	d	e	r
a	u	s	l	a	n	d
s	p	r	e	s	s	e

C

3	5	2	7	6	1	4
d	e	r	f	r	a	n
z	o	e	s	i	s	c
h	e	a	u	s	s	e
x	m	i	n	i	s	t
e	r	e	r	k	l	a
e	r	t	e	v	o	r
d	e	m	r	a	t	d
e	r	r	e	p	u	b
l	i	k	d	a	s	n
e	u	e	a	b	k	o
m	m	e	n	m	i	t
d	e	m	s	a	a	r
g	e	b	i	e	t	

Box II

A

4	5	2	6	1	3
a	s	s	s	f	t
e	t	r	e	a	i
e	g	e	e	d	z
h	n	e	n	r	e
o	n	c	e	t	i
e	d	i	e	o	e
m	r	g	n	l	n
r	i	s	i	p	s
n	a	f	s	u	n
m	e	i	g		

B

4	5	2	6	1	3
a	s	s	s	a	e
n	s	r	e	a	i
s	o	s	r	d	z
h	n	e	h	a	s
n	c	e	t	c	r
d	e	s	o	e	m
r	v	u	p	r	i
s	i	r	d	a	s
f	s	u	n	p	r
l	e				

C

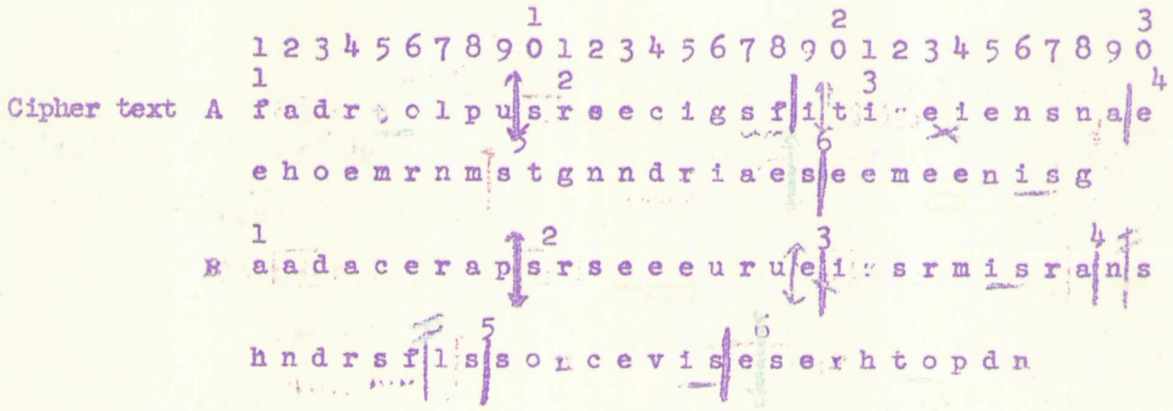
4	5	2	6	1	3
a	s	s	s	l	o
t	u	s	k	i	a
t	x	e	a	i	e
t	m	r	k	e	e
m	b	d	z	h	m
e	e	d	e	l	e
m	d	g	n	c	e
t	a	r	d	b	n
s	t	r	e	o	e
m	r	r	e	r	i
u	m	e	e	r	i
s	i	k	v	a	p
a	b	m	a	e	f
s	u	n	x	e	r
e	d	a	n	s	i

II A 1b - 1

TOP SECRET

Doc ID: 6592460

TOP SECRET



1-place chain count (digraphic count)

	Cipher text A	Cipher text B
a	d e e	a a d c p a
b		
c	i	c e e
d	r r	d a r n
e	e c i n e h m s e n e n	e r e e u i v s r
f	a i	f l
g	s n	g
h	o	h n t
i	g t r e a s	i r s s
j		j
k		k
l	p	l s
m	r s	m u
n	s a m n d e i	n s d c
o	l e	o n p
p	u	p s d
q		q
r	t e n i	r a u m a s h
s	r f n t e g	s e r r h f s o e e
t	o i g	t o
u	s	u r e
v		v i
w		w
x		x
y		y
z	e	z s

II A l b - 2

TOP SECRET

Doc ID: 6592460

Matching Columns:

1) Position of columns 1,2,6 on the basis of their depth in A and B.

Column lengths	A	10	10	10	10	9	9
" "	B	10	10	9	9	9	9
Position						1	1
					2	2	
					6	6	

II Alb3

2) Sequence of columns on the basis of like digraphs:

Digraph	to	Column	A	and	B	Sequence of columns: 6 1	or	6 · 1
"	st	"	A 2	"	B 4	4 2		4 · 2
"	is	"	A 6	"	B 3 / B 5	3 6 5 6		3 · 6 5 · 6
"	ee	"	A 6	"	B 2	2 6		2 · 6

3) Joining 1) and 2)

A	10	10	10	10	9	9
B	10	10	9	9	9	9
			2	6		
		3				
		5		6		
	4		2			

4) The like positioned digraphs ad in column 1 and iv in column 3 mean that columns 1 and 3 are adjacent.

Hence: $\begin{matrix} 4 & 5 & 2 & 6 & 1 & 3 \\ & & & & 3 & 1 \end{matrix}$

II A - 1 b - 3

TOP SECRET

Matching the cipher columns

A

4	5	2	6	1	3
a	s	s	s	f	t
e	t	r	e	a	i
e	g	e	e	d	z
h	n	e	n	r	e
o	n	c	e	t	i
e	d	i	e	o	e
m	r	g	n	l	n
r	i	s	i	p	s
n	a	f	s	u	n
m	e	i	g		

or

4	5	2	6	3	1
a	s	s	s	t	f
e	t	r	e	i	a
e	g	e	e	z	d
h	n	e	n	e	r
o	n	c	e	i	t
e	d	i	e	e	o
m	r	g	n	n	l
r	i	s	i	s	p
n	a	f	s	n	u
m	e	i	g		

B

4	5	2	6	1	3
a	s	s	s	a	e
n	s	r	e	a	i
s	o	s	r	d	z
h	n	e	h	a	s
n	c	e	t	c	r
d	e	e	o	e	m
r	r	u	p	r	i
s	i	r	d	a	s
f	s	u	n	p	r
l	e				

or

4	5	2	6	3	1
a	s	s	s	e	a
n	s	r	e	i	n
s	o	s	r	·	d
h	n	e	h	s	a
n	c	e	t	r	c
d	e	e	o	m	e
	v	u	p	i	r
s	i	r	d	s	a
f	s	u	n	r	p
l	e				

A

a	s	s	s	f	t	e	t	
r	e	a	i	e	g	e	e	
d	z	h	n	e	n	r	e	o
n	c	e	t	i	e	d	i	
e	o	e	m	r	g	n	l	n
w	i	s	i	p	s	n	a	
f	s	u	n	m	e	i	g	

B

a	s	s	s	a	e	n	s	
r	e	a	i	r	o	s	r	
d	z	h	n	e	h	a	s	
n	c	e	t	c	r	d	e	
e	o	e	m	r	v	u	p	
r	i	s	i	r	d	a	s	
f	s	u	n	p	r	l	e	

II A - 1 b - 4

TOP SECRET

2. Matrix transposition with grille.

(Würfel mit Raster)

In many respects the combination of a simple matrix transposition with a grille works out in much the same fashion. The procedure consists in marking off in the matrix the open squares of a superimposed grille and not using them for encipherment. Since the grille is neither slid nor turned, there are no rules or limitations regarding the arrangement of the grid cells. The text to be enciphered is entered horizontally in the matrix omitting the cells blocked by the grille and is then taken out by columns according to a numerical key.

In Appendix II A 2 two plain texts A and B have been enciphered with the same matrix in the same grille. The blocked cells of the grille extend only to a certain depth which is less than the utilized depth of the matrix. The two texts have two fairly long parallel passages.

If a sufficient number of grille cells are blocked and if their distribution is unsystematic, it results that a matching of transposition columns by plain digraphs is no longer possible in the grille area. A single cipher text enciphered by this system is therefore secure against unauthorized decipherment if the blocked cells are distributed in sufficient density over the entire matrix. Only when several texts in the same key and of the same length are available is solution possible. The method corresponds to that used for double transposition.

If several messages in the same key but differing in length are available, relatively short parallel passages in the plain text will no longer be recognized in the several cipher texts. Only parallel passages with a length exceeding the width of the matrix can appear as parallel passages in the cipher text, provided they are like positioned or if the grille cells correspond at the two positions. When such relatively long parallel passages in the plain text as "der französische Aussenminister" of our example are in phase, then they appear in the

cipher text (see parallel passages framed in brown in cipher text A and B on sheet 2) in the same position when the cipher texts are identical in length and in nearly the same position when the cipher text are of different length. The similarity of position consists in the fact that the sequence of the parallel passages is the same in the two cipher texts and that their intervals stand in a definite relation to the total length of the messages. The number of like positioned parallel passages corresponds to the number of columns in the matrix if their length is adequate. If the parallel passage stands at the beginning or end of the plain text, then the parallel passages form the beginnings or ends of the columns of the cipher text.

When the parallel passages in the plain text, e.g. "der nächsten Aussenministerkonferenz" in our example, are not in phase, then the parallel passages in the cipher text appear in a deviating sequence. Their number may correspond to the width of the matrix; their intervals stand in relation to the message lengths.

If the columns of cipher text A, whose number and length in the present case are given by the parallel passages, are juxtaposed as shown in the upper left corner of sheet 3, we get the characteristics of the grille-matrix:

1. Deviation of more than one element in the depth of the column;
2. The parallel passages of the plain text belonging to the parallel passages of the cipher text also show differences of length in excess of one element, insofar as they have been influenced by the grille.

By merely looking at the columns in the upper left corner of sheet 3 we can see that in this example the grille affected only the upper part of the matrix. A comparison

	In columns	1	2	3	4	5	6	7	8	9
1)	Of the length of the repeats framed in brown	3	3	4	4	4	4	3	3	2
2)	Of the interval to the next parallel passage	3	1	2	3	2	3	3	2	2
3)	Of the length of the repeats framed in green	3	3	4	3	4	3	3	3	3
4)	Of the interval to the end of the column	4	4	4	5	4	4	4	5	4

Doc ID: 6592460

shows on the basis of the differences in length that the repeats framed in brown and also the text ahead of the repeats framed in green lie in the area of the grille while the remainder of the message was enciphered with a simple matrix.

Corresponding to the lower portion (no longer influenced by the grille) the columns can be arranged for the moment in three groups (sheet 3 at the upper right):

I.	Length of the repeat framed in green	4 elements
	Length to the end of the column	4 elements
II.	Length of the repeat framed in green	3 elements
	Length to the end of the column	5 elements
III.	Length of the repeat framed in green	3 elements
	Length to the end of the column	4 elements

If the top of the repeats framed in green are brought to the same level, the lower half of the grill-matrix, which is not influenced by the grille, is yielded.

Taking into account the c and h standing on the same level we get the sequence 5 3 8 4 7 1 (middle of sheet 3 at the left). For the remaining three columns the sequence can be determined by the resulting plain text.

After the sequence of columns and the lower part of the plain text in the matrix have been recognized, it is possible to reconstruct the grille portion row by row working up from the bottom in such fashion that all elements which do not fit into the plain text are pushed up and the vacant cells are marked as grille cells (see middle of sheet 3 at the right).

Even easier is the reconstruction of the matrix on the basis of the parallel passages not in like position (framed in green). When the pairs of columns which are connected either in the two texts (in our example A and B) or within the same matrix by a parallel passage which is not like positioned, then a transition sequence can be derived (bottom of sheet 3) which either contains

Doc ID: 6592460

the numerical key of the matrix or from which this key can be derived since these transition sequences are related to one another like the substitute slide of the short slide.

The two methods of solution given are, however, ways of solving the simple matrix transposition which can only be used insofar as the grille does not extend over the total depth of the matrix employed or the grille is so little developed that parallel passages of the plain text can be recognized even when not in phase. Consequently these types of solution do not affect the security of the grille-matrix substitution as such.

TOP SECRET

```
                                1                   2                   3
          1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0

Plain text: D E R F R A N Z O E S I S C H E A U S S E N M I N I S T E R
            B E A B S I C H T I G T A U F D E R N A E C H S T E N A U S
            S E N M I N I S T E R K O N F E R E N Z A U C H D E N S C H
      A     U M A N P L A N Z U R S P R A C H E Z U B R I N G E N X
                                                          118 elements

            D E R F R A N Z O E S I S C H E A U S S E N M I N I S T E R
            E R K L A E R T E A U F D E R G E S T R I G E N P R E S S E
            K O N F E R E N Z D A S S E R I N S E I N E N B E S T R E B
      B     U N G E N U M D I E E R H A L T U N G D E S F R I E D E N S
            N I C H T N A C H L A S S E N W E R D E X E R E R H O F F E
            S I C H V I E L V O N D E R N A E C H S T E N A U S S E N M
            I N I S T E R K O N F E R E N Z X
                                                          197 elements
```

Transposition box with grille

```
      5 3 8 4 7 1 9 6 2
    1 D . E R F R . A N
A   2 Z O . E S . I S C
    3 . H E A . U S S .
    4 E N M I N I . S T
    5 E R . B E A B S I
    6 C H T I G T . A .
    7 U F D E R N A E .
    8 C H S T E N A U S
    9 S E N M I N I S T
   10 E R K O N F E R E
   11 N Z A U C H D E N
   12 S C H U M A N P L
   13 A N Z U R S P R A
   14 C H E Z U B R I N
   15 G E N X
```

```
      5 3 8 4 7 1 9 6 2
    1 D . E R F R . A N
B  22 Z O . E S . I S C
    3 . H E A . U S S .
    4 E N M I N I . S T
    5 E R . E R K L A E
    6 R T E A U F . D .
    7 E R G E S T R I .
    8 G E N P R E S S E
    9 K O N F E R E N Z
   10 D A S S E R I N S
   11 E I N E N B E S T
   12 R E B U N G E N U
   13 M D I E E R H A L
   14 T U N G D E S F R
   15 I E D E N S N I C
   16 H T N A C H L A S
   17 S E N W E R D E X
   18 E R E R H O F F E
   19 S I C H V I E L V
   20 O N D E R N A E C
   21 H S T E N A U S S
   22 E N M I N I S T E
   23 R K O N F E R E N
   24 Z X
```

II A 2 - 1

TOP SECRET

Doc ID: 6592460

TOP SECRET

Cipher text

```
                1                   2                   3
    1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0
    R U I A T N N N F H A S B N C T I S T E N L A N O H N R H F
    H E R Z C N A E R E A I B I E T M O U U U Z X D Z E E C U C
A   S E N S A C G A S S S S A E U S R E P R I F S N E G R E I N
    C M R U E E M T D S N K A H Z E N I S B A A I E D N P R
    ---------------------------------------------------------
    R U I K F T E R R B G R E S H R O I N A I E N C T E E Z S T
    U L R C S X E V C S E N O H N R T R E O A I E D U E T E R I
    N S N K X R E A I E A E D F S C U E G E A W R H E E I N D Z
B   E E R E G E D E R M T I H S E S O H E R Z A S S S A D I S N
    N S N A F I A E F L E S T E F S N R U S R E E N N E D N C E
    H V R N N F E E M E G N N S N B I N D N N E C D T M O I S L
    R S E I E E H S N L D F E A U S R
    ---------------------------------
```

Digraphic count of cipher texts "A" and "B"

	A	B
A	T S N I C S E H A I	I I I E W S D F E U
B	N I A	G I
C	T N U S G M	T S S U E D
D	Z S N	U Z E I N N T F
E	N R R A T E C N U	R S N E Z V N O D T R A A P G A E I E R
	P G I E M N D	G D R S I E H A R F S F E N D H E M G C
F	H H S	T S I L S E E
G	A R	R E E N
H	A N F E E Z	R N E S E V S
I	A S B E F N S E	R N E E N E N H S A N S E
J		
K	A	F X
L	A	R E R D
M	O R T	T E O
N	N N F C L O R H	A C O R S K D N S A R N
	S E C K I P	E C N F N S B D N E L
O	H U	I H A H I
P	R R	F
Q		
R	U H Z E E I E V	U R B E O C T E I E H E M Z U E N S
S	B T E A S S S A R N N B	H T X E N C E O S S A N T N R N L E N R
T	N I E M D	E E U R E I E M
U	I U U Z C S E	I L E E S S
V		C R
W		R
X	D	E R
Y		
Z	C X E E	S E A

TOP SECRET

A	1	2	3	4	5	6	7	8	9
	R	N	O	R	D	A	F	E	I
	U	C	H	E	Z	S	S	E	S
	I	T	N	A	E	S	N	M	B
	A	I	R	I	E	S	E	T	A
	T	S	H	B	C	S	G	D	A
	N	T	F	I	U	A	R	S	I
	N	E	H	E	C	E	E	N	E
	F	L	E	T	S	U	I	K	D
	H	A	R	M	E	S	N	A	N
	A	N	Z	O	N	R	C	H	D
	S		C	U	S	E	M	Z	R
	B		N	U	A	P	R	E	
			H	U	C	R	U	N	
			E	Z	G	I			
				X					

3	5	4	8	1	2	6	7	9
O	D	R				A		
H	Z	E		R	S	S	F	
N	E	A	E	U		S	S	
R	E	I	E	I	N	S	N	I
(H)	(C)	B	M	A	C	S	E	S
F	U	I	T	T	T	A	G	B
(H)	(C)	E	D	N	I	E	R	A
E	S	T	S	N	S	U	E	A
R	E	M	N	N	T	S	I	I
Z	N	O	K	F	E	R	N	E
(C)	S	U	A	(H)	N	E	(C)	D
N	A	U	(H)	A	L	P	M	N
(H)	(C)	U	Z	S	A	R	R	P
E	G	Z	E	B	N	I	U	R
		X	N					

A	5	3	8	4	7	1	2	6	9
				B	E	A		S	
	(G)	(H)	T	I	G	T		A	B
	U	F	D	E	R	N	I	E	A
	(C)	(H)	S	T	E	N	S	U	A
	S	E	N	M	I	N	T	S	I
	E	R	K	O	N	F	E	R	E
	N	Z	A	U	(C)	(H)	N	E	D
	S	(C)	(H)	U	M	A	L	P	N
	A	N	Z	U	R	S	A	R	P
	(C)	(H)	E	Z	U	B	N	I	R
	G	E	N	X					

A	5	3	8	4	7	1	9	6	2
				R				A	
				E				S	
				A	X	U	S	S	X
	E	N	M	I	N	I	S	S	T
	E	R	M	B	E	A	B	S	I
	C	H	T	I	G	T	B	A	E
	U	F	D	E	R	N	A	E	X
	C	H	S	T	E	N	A	U	S
	S	E	N	M	I	N	I	S	T
	E	R	K	O	N	F	E	R	E
	N	Z	A	U	C	H	D	E	N
	S	C	H	U	M	A	N	P	L
	A	N	Z	U	R	S	P	R	A
	C	H	E	Z	U	B	R	I	N
	G	E	N	X					

Parallel passages not in like position are found in cipher texts "A" and "B"

In column 1 2 3 4 5 6 7 8 9 of text B
" " 9 5 8 7 3 2 1 4 6 " " A

Transition sequence: 1 9 6 2 | 5 3 8 4 7 1 9 6 2 | 5 3 8 4 7

II A 2- 3

3. Substitution with short transposition key.

(Cäsar mit Umstellzahl)

When a text enciphered by simple substitution is shifted in the second operation using the transposition key of limited length, the count shows the normal distribution of a substitution system but solution as a simple substitution is impossible. A correct analysis can only be reached through the supplemental evaluation of the parallel passages on the basis of detached elements characteristic of the short key transposition.

Insofar as parallel passages do not appear in the cipher text, either because there are none in the plain text or because they no longer appear due to the transposition, the system can be regarded as secure. It also results that the security of the system increases with the length of the transposition key. The amount of traffic which can be enciphered with security stands therefore in direct relation to the length of the transposition key.

4. Substitution with matrix transposition.

(Cäsar mit Würfel)

If a text enciphered by substitution is then transposed, the count of the cipher text will show the frequencies of the substitution but will not show the parallel passages characteristic of the simple substitution provided the matrix width is so chosen that any existing plain text parallel passages will not extend beyond the width of the matrix. Even the frequency of specific digraphs characteristic of the substitution will drop out. Solution as a substitution is impossible until the natural linguistic sequence is restored in the cipher text. Furthermore solution as a simple transposition will not be possible because there is no criterion for the correctness of juxtaposed digraphs and trigraphs. Analysis of the cipher text will only be possible if cipher texts in the same key contain parallel passages which can only arise from parallel passages in the plain text with a length greater than the width of the matrix, or when errors have been made in encipherment which may give the analyst clues regarding the system used. Such errors include a wrong use of the numerical key or the omission of elements when enciphering which makes necessary a repetition of the message. If this repetition is enciphered with the same matrix, then a comparison of the two cipher texts may reveal the number and length of the column and allow deductions as to the system.

Consequently this combination of substitution and transposition affords good security as long as traffic is light and the alphabets and matrices can be changed often enough and provided care is taken when enciphering to prevent the occurrence of parallel passages longer than the width of the matrix in messages in the same key.

5. Code with short transposition key.

(Code mit Umstellzahl).

When a code text is transposed by a key, the value of the combination depends on the ratio of the length of the code group to the length of the key. If the length of the key is the same as the length of the code group, there is no essential increase in the difficulty of solution because the frequency of the individual groups and the parallel passages remain unchanged and frequent groups can be recognized as such in the transposed form.

If, on the other hand, the length of the code group and the length of the key have no common factors, the product of these lengths gives the interval at which genuine parallel passages can appear for the first time. Hence the security of the system increases with the length of the key.

Even before parallel passages appear it may be possible to analyze the system by making a count of the individual elements. As a rule a cipher text produced with a particular code will show, after a certain amount of traffic has accumulated, a curve characteristic of that code for the frequency of the single elements of which it is composed. If, for instance, the most frequent groups of a 4-digit code are 0081 0880 7880 9009 8088 etc. a count of the individual elements 0 to 9 will show marked peaks for 8 and 0.

6. Code with matrix transposition.

(Code mit Würfel)

From an analytic point of view the combination of code and transposition works out in much the same way. Since with the code of 10,000 or more groups relatively long parallel passages are rare, it is possible to avoid recognizable parallel passages in the cipher text if the matrices have a certain minimum width. From the frequency curve for the single elements some idea of the code is obtained and hence a recognition of the fact that a code with transposition is involved. If a message which was originally transmitted with errors is repeated, this may permit recognition of the use of matrix transposition.

If the matrices and key numbers are changed often enough and if proper precautions are taken, this system affords a very high degree of security. If the code is unknown, then even bad errors in encipherment will permit recovery of this or that matrix only in exceptional cases. But as long as these cases are the exception and the keys are changed frequently it will not be possible to accumulate enough material to solve the unknown code.

In spite of the relatively high degree of security such a system can only be used in the long run with low traffic density because the frequent sources of error and the time required would become too burdensome.

7. Polyalphabetic substitution with short transposition key or with matrix. (Spaltencäsaren mit Umstellzahl oder Würfel)

Inasmuch as the proper use of polyalphabetic substitution alone affords a high degree of security for a large amount of traffic, the combination of a polyalphabetic substitution (Springcäsar or Spaltencäsar) with a short transposition key or a matrix is rare in actual practice because the expenditure of time involved by the second encipherment is generally regarded as superfluous.

This does not argue against the use of the combination since a good substitution system can only gain in security by reencipherment with a transposition system.

The combination of two basic systems mentioned in the foregoing chapters virtually exhausts the possibilities. It has been shown that reencipherment usually results in a noticeable gain in security. This explains the relatively wide use of such systems despite the increased expenditure of time. Other combinations which are theoretically possible are very seldom actually used whether it be that the increase in security is not significant or that the cost in time is too great.

Section B.

Superenciphered Systems

(Überschlüsselte Verfahren)

Special systems have been developed for subjecting the text produced by a basic system, the so-called intermediate text (Grundtext), to another encipherment or superencipherment, so that from the intermediate text the final text arises. These systems of superencipherment differ from the basic systems through the fact that by means of the superencipherment a plain text cannot be transformed into a cipher text directly but the superencipherment can only be applied to an intermediate text produced by a basic system.

1. Encipherment by substitution table.

Tauschtafelüberschlüsselungen.

If the text produced by a digit code is so changed that

from a	0 1 2 3 4 5 6 7 8 9
a	4 3 6 9 2 8 0 5 1 7

always results, then beyond doubt a 1-place substitution is involved which is much like a Cäsar. But since here we do not have a plain sequence standing over against a cipher sequence but rather a cipher sequence II, what is involved is a superencipherment system which has become known under the designation Tauschtafel (substitution table).

Such one-place tables may be used as letter substitution tables or digit substitution tables for the superencipherment of the text produced by a letter or digit code.

As long as the substitution tables are not changed very often, the result, in respect to increased security, is only slight.

For instance, if the 1-place substitution table reads as follows:

Cipher sequence I	0 1 2 3 4 5 6 7 8 9
Cipher sequence II	6 3 9 1 5 0 8 2 4 7

and the code text to be enciphered shows the following groups:

1344 4314 0878 4488 5348 4408 1348 . . . . ,

then the superenciphered text II

3155 5135 6424 5544 0154 5564 3154 . . . . . .

would agree with the intermediate text in structure just as a simple Cæsar fails to conceal the structure of the plain language. Even without picking out such constructive parallel passages and evaluating the results, certain frequent groups with a characteristic group structure could readily be reduced to one another. To some extent a reduction would be possible solely on the basis of the frequency of the individual elements.

On the other hand, if analogous to the Springcæsar or Spaltencæsar several 1-place substitution tables are used in unsystematic sequence and at short intervals, such a superencipherment would cause both parallel passages and passages of similar construction to disappear entirely so that any solution of the substitution tables and hence any solution of the cipher text becomes impossible, provided the same sequence of substitution tables is not used repeatedly.

The 1-place substitution table for enciphering a digit code may also have letters in cipher sequence II so that the digit text becomes a letter text. Since in this case there are 26 elements in cipher sequence II against 10 elements in cipher sequence I it is possible to use variants. With the table:

Cipher sequence I	0 1 2 3 4 5 6 7 8 9
Cipher sequence II	c d i g a h e j b f
	t k q v r n s l m p
	u - o - w z x - y -

the digit group "2045" may be replaced in the superenciphered form by the following groups:

i c a h	i c r h	i c w h
i c a n	i c r n	i c w n
i c a z	i c r z	i c w z
i t a h	i t r h	i t w h
i t a n	i t r n	i t w n
i t a z	i t r z	i t w z
i u a h	i u r h	i u w h
i u a n	i u r n	i u w n
i u a z	i u r z	i u w z
q c a h	q c r h	q c w h
q c a n	q c r n	. . . . etc.
o c a h	o c r h	o c w h
o c a n	o c r n	. . . . etc.

Hence for each 4-digit group there are from 2^4 to 3^4, i.e. from 16 to 81 possibilities of encipherment so that even rather long parallel passages can be so enciphered each time as to get such a different structure so that recognition of the parallel passage may become a difficult or even impossible task and no reduction of the tables can be achieved if they are changed often enough.

What has been said about the effect of the 1-place substitution table holds true in increased measure for 2, 3 and more place tables. The greater the number of substitution table groups becomes which have to be reduced to one another, the more traffic will be required before any reduction can be attempted. If the tables are changed so promptly that enough material for reduction of any table can never be secured, then the security of the superencipherment is guaranteed.

There is the additional fact that in the superencipherment of 5-place code groups by 3-place substitution tables any reduction on the basis of constructive similarities of the individual groups may be difficult, especially since parallel passages of the intermediate text I only appear in the final text II when they are in phase.

If a multi-place substitution table is used not to encipher the intermediate text serially but column by column when written out in appropriate form, then each three-place group of the table might encipher three single elements from three different code groups, even covering different positions in the several groups.

If substitution tables are combined with a simple transposition of the intermediate text in this way, clues for any reduction can be eliminated, even when there is a rather large amount of traffic - say with rare change of key - to such an extent that any solution of the substitution tables becomes impossible.

2. Additive

Die Überschlüsselungszahl.

For digit codes a special method of encipherment has been developed which consists in the addition of a so-called Überschlüsselungszahl (additive) to the text produced by the code. Almost without exception symbolische Additionsweise (addition modulo 10) is used, i.e. the tens resulting from the addition of single digits are disregarded. Thus if we add

to code text	0268343246914934ll
the additive sequence	9437612349437612 34
the final cipher text II reads	9695955585341546 45.

If the additive is 1-place or if the number of places coincides with the number in the code group, the following situations result:

Code text:	0513 2419 5506 8129 0513
Additive:	6666 6666 6666 6666 6666
Cipher text II	6179 8075 1162 4785 6179

or

Code test:	0513 2419 5506 8129 0513
Additive:	2583 2583 2583 2583 2583
Cipher text II	2096 4992 7089 0602 2096.

In both cases, all the repetitions of the code text are preserved and in addition the differences between the individual code groups remain unchanged. If the basic code is known to the unauthorized cryptanalyst, the enciphered text II can be reduced to the basic code on the basis of the unchanged differences between the groups.

These differences are also determined symbolically (mod 10). The question as to which of two code groups compared is the minuend or the subtrahend is settled as a matter of principle according to the least possible difference between two numbers. For instance, if the numbers 8129 and 0134 are to be considered, then symbolic subtraction yields these possible answers:

8129		0134
0134		8129
8095	and	2015.

Of these two values, which are complementary with respect to 0000, we consider only 2015 as the least difference. If the code groups under consideration read:

8129	3173
3173	8129
5056	5054,

then it is only the last place which determines the direction in which the difference is to be taken. In certain border line cases, e.g. with the groups:

8129	8129	8129	8129
8124	3174	8629	3679
0005	5055	0500	5550

we get the same difference both ways, irrespective of which group is taken as the minuend.

By determining the least differences between the groups of the cipher text it is easy to recognize the use of an additive with a known code. Reduction to the basic code is then simple.

If the basic code is not known, then the enciphered code groups can be reduced to one another starting with any arbitrary assumption in case of a long additive or of a change of additive, but collectively they only form a relative code. If the basic code has 4-digit groups, its groups differ from those of the relative code by a constant difference which lies between 0000 and 9999. Therefore a 4-place basic code is only

one among 10,000 possible relative codes. If the additive is neither a single digit nor of the same length as the basic code group, a period results which is equal to the least common multiple of the length of the additive number and the number of digits in the code group.

Appendix II B 2 shows an intermediate text I consisting of 5-digit groups which is transformed into the final cipher text II by the addition of a recurrent 6-place additive. The numerous parallel passages of intermediate text I no longer appear in cipher text II save for those standing at an interval of 30 or some multiple thereof (i.e. the least common multiple of the 5 digits of the code group and the 6 digits of the additive). These parallel passages with the length of the code group or a multiple thereof occurring at regular intervals which are likewise the length of the code group or a multiple thereof, do not reveal the frequency characteristics of plain code and are indicative of the fact that additive encipherment is present.

Since the differences of the enciphered code groups in the several columns of the appendix were not changed by the addition of the additive number, we may infer from like differences between two groups of one column and two groups of another column that the groups in question may have been alike in the intermediate text I.

Consequently on sheet 1 all the least differences have been given column by column with an indication of the direction in which they were formed. At the top of sheet 2 these have been tabulated with an indication of the position of the groups which were differenced.

In all cases where the difference of two groups in one column corresponds to the difference of two other groups in another column we can now make the assumption that the same two groups of the basic code are involved. Even though enciphered groups often show like differences although the underlying code groups are not the same, this course may be taken because the assumption will prove correct in the majority of cases.

Thus if the difference of the groups 30625 01420 in column 1 rows a and c, of the groups 22133 93938 in column 4 rows d and a, and of the

the groups 59477 20272 in column 6, b and d is in each case 39205, then it is possible to assume that the minuends and subtrahends correspond to the same groups of the basic code. If we add 00000 to the groups of column 1, 18592 to the groups of column 4 and 81258 to the groups of column 6, we reduce the potentially corresponding groups of columns 1, 4 and 6 to the values of column 1. The numbers added in this way to the groups of a column are called Reduktionszahlen (reduction numbers), because with them the groups of the various columns can be reduced to a common relative code. These reduction numbers are found as differences between the minuends and subtrahends which together yield the same least differences.

At the bottom of sheet 2 the like least differences have been evaluated in this fashion and the resulting reduction numbers obtained. A comparison of the reduction numbers with one another shows that they confirm one another with the exception of the reduction number belonging with least difference 52962 which means that in this case the assumption that like code groups yielded the same difference was false.

After cipher text II has been reduced to a relative code by the aid of the reduction numbers obtained, the reduced text shows the same repetitions as the original intermediate text I.

If the code is unknown and the additive is random, then we have gone as far as possible with the solution of the superencipherment. Solution of this relative code could be attempted as soon as enough material has been reduced.

If, on the other hand, the basic code is known, then it is well to reduce the messages to the basic code by adding the reduction number which is easily found.

If the same basic code is enciphered successively with different additives, it is always necessary to reduce to the same relative code. For this purpose and for all reductions of enciphered text of the same basic code it is very advantageous to use a so-called Differenzenkatalog (table of differences). This table of differences contains the

differences between all frequently-occurring groups of the same code. Under the same difference are entered those code groups which together produce this difference. It is well to use several tables side by side; one will contain only the differences between the most frequent code groups; a second, the difference between the most frequent and less frequent code groups, and the third, only the differences between the less frequent code groups. On the other hand, if one prefers to have a single catalogue, the groups yielding the same difference may be arranged in the order of their frequency or notations regarding the frequency of the groups may be made, say with the letters a, b, c.

Using a good difference table, columns with a depth of only four or five groups can be reduced to one another even in the case of an unknown code. After solving the code even lesser depths can be reduced to one another with the aid of the table.

When, as in the present example, the additive period of 30 elements has a length equal to the product of the number of digits in the code and the number of digits in the additive, it is possible to recognize the structure of the additive from the reduction numbers for the various columns by finding the intermediate differences (Zwischendifferenzen) between the several reduction numbers. At the bottom of sheet 3 we find the repeated number 4 2 9 8 5 2 which results from the intermediate difference of adjacent column reduction numbers and is constantly repeated with cyclic displacement.

A comparison of 4 2 9 8 5 2 with the original number 3 5 4 2 7 9 shows that the number 4 2 9 8 5 2 is made up of the difference of adjacent elements of the original additive. Hence from the number 4 2 9 8 5 2 we can derive 10 additives with the same relative construction of which one is the original additive. Since the additive and the reduction number, insofar as both are used in the additive procedure, are complementary, the reduction number must be formed according to the complement to 4 2 9 8 5 2, i.e. according to the number 6 8 1 2 5 8.

At the bottom of sheet 3 of the appendix are found the resulting reduction numbers which lead to one of ten possible relative codes. On sheet 4 the encoded text I has been recovered with the aid of the new reduction numbers.

As this method of solution shows, an additive of limited length can not afford adequate security when used with the code because the differences in the single columns permits recognition of the original code groups.

On the other hand, if the additive is so used that it is not possible to match up by columns the code groups enciphered with the same additive number, then a solution is out of the question.

Consequently, if an additive is to be used more than once, it will be necessary to subdivide the additive, let us say by row and column in a table, so that the additive is taken out by a different route each time. As long as the same route is not used frequently this will prevent lining up the text by columns.

Of course the safest way of using additive is to use it once only. For this purpose one can either use for each message to be enciphered a new additive sequence as long as the message, or an additive of unlimited length may be used starting each message where the last ended.

As equivalent to a one-time additive we may regard several uses of the same additive sequence if the starting points are chosen so as not to correspond to the length of the code groups, e.g. if an additive sequence divided into 5-digit groups is applied to 5-digit code groups so that the starting point will be first on the first element, next on the second element, then on the third, fourth, and fifth element of a specific group.

It may be appropriate to mention at this point the way in which additive sequences of considerable length were derived - originally by the Russians - from a short key number without repetition of the additive. This method is primarily suitable for emergency keys or agent systems since the basic material required is little or none.

In Appendix II B 2 e are shown the beginnings of several additive sequences derived from various key numbers. Adding mod 10 the first and second elements of the key number gives the first element of the additive; adding the second and third elements of the key number gives the second element of the additive, etc.; finally adding the last element of the key number and the first element of the additive gives the next element of the additive and the process is now continued starting at the beginning of the additive sequence.

Examples 1 to 3 and 4 to 6 show that even the slightest deviation in two otherwise like key numbers very quickly affect the additive sequences so greatly that they soon show no agreement despite the almost identical key numbers. (If two key numbers agree in x consecutive elements, this agreement shows up in x - 1 sections of the length x for (x-1) - (x-2) - (x-3) - .....(x-x) elements.

Examples 7 to 9 show how the combination of two key numbers into a single key works out.

Example 10, on the other hand, shows how an error in deriving the additive from the key multiplies. Row a shows the correct additive, row b, the change occasioned by the omission of one element, and row c, the effect of a falsely computed element of the additive. Example 11 shows how a mistake in the key number itself works out. The error and the resulting deviations in the additive have been marked by an x.

These last two examples lead to the conclusion that this derivation of the additive sequence - simple as it at first appears - must be limited in practice because it is not everywhere possible to make the inevitable careful check on the accuracy of the additive before it is used.

Repeated use of the same additive sequence derived in this fashion must also be greatly limited for security reasons since additives thus derived show regularities, as is revealed by the study in Appendix II B 2 e sheet 2 of additives produced by 2- and 3-place key numbers. These regularities include the following characteristics:

1.) If 0 and 5 have regular intervals within the additive sequence, e.g. with the numbers 01, 04, 013, 026 then the second half of the additive consists of the complements of the first half.

2.) If 0 and 5 have no regular intervals within the additive sequence, there is a second additive number resulting from the complement of the first additive sequence, e.g. with the key numbers 001 and 009, 002 and 008, 003 and 007, 004 and 006.

3.) Various additive sequencem can be derived from an additive sequence by symbolic multiplication, e.g. in the case of key numbers 01, 04 and 05 or 001, 002, 003, 004, 005, 006, 007, 008, 009 or 013 and 026.

4.) Each 0 in the additive leads to the formation of pairs at definite intervals which depend on the length of the key. If the pairs are represented by x and the intervals by dots, we get for 3-digit keys the two regularities: 0x..xxx and 0...xx

In the tabulation in the squares on sheet 1 and sheet 2 we can see by the colors which key numbers lead to the same additive number with cyclic displacement. For instance, if the additive derived from the key number 003 begins with 0333669251, etc., the numbers 033, 333, 336, 366, 669, 692, etc. as key numbers yield the same additive; hence all the key numbers connected through the same additive number have been entered in the same color in the squares.

Doc ID: 6592460

~~TOP SECRET~~

Column reduction number	00000	42985	66173	18592	93734	81258	
Cipher text I	05208	13276	35942	76003	89165	13276	
Additive	35427	93562	79354	27935	42793	54279	
Cipher text II	30625	06718	04296	93938	21858	67445	
Reduced text	30625	48693	60369	01420	14582	48693	a
Cipher text I	28238	13276	92463	22216	13363	05208	
Additive	35427	93542	79354	27935	42793	54279	
Cipher text II	53655	06718	61717	69141	55056	59477	
Reduced text	53655	48693	27880	77633	08780	30625	b
Cipher text I	76003	35942	25139	13363	28238	65138	
Additive	35427	93542	79354	27935	42793	54279	
Cipher text II	01420	28484	94483	30298	60921	19307	
Reduced text	01420	60369	50556	48780	53655	90555	c
Cipher text I	89165	25139	87804	05208	42216	76003	
Additive	35427	93542	79354	27935	42793	54279	
Cipher text II	14582	18671	56168	22133	84909	20272	
Reduced text	14582	50556	12221	30625	77633	01420	d
Cipher text I	13276	76003	76003	42216	89165	92463	
Additive	35427	93542	79354	27335	42793	54279	
Cipher text II	48693	69545	45357	69141	21858	46632	
Reduced text	48693	01420	01420	77633	14582	27880	e

Difference		1	2	3	4	5	6
	a b	23030↓	00000.	43589↑	34897↑	34208↓	18078↑
	a c	39205↑	22776↓	10813↑	47360↓	49173↓	52962↓
	a d	26143↑	12963↓	52952↓	39205↓	47959↑	47273↑
	a e	18078↓	47273↑	41161↓	34897↑	00000.	21813↑
	b c	52235↑	22776↓	33776↓	39953↑	15975↓	40170↑
	b d	49173↑	12963↓	15669↑	47018↑	39953↓	39205↑
	b e	15062↑	47273↑	26460↑	00000.	34208↑	13845↑
	c d	13162↓	10813↑	48335↑	18165↑	24088↓	11975↓
	c e	47273↓	41161↓	51975↓	39953↓	49153↑	37335↓
	d e	34111↓	51975↓	11801↑	47018↓	47959↓	26460↑

II B 2 b - 1

~~TOP SECRET~~

Doc ID: 6592460

TOP SECRET

Count of least differences:

00	
1	
2	
3	
4	
5	
10	873cd2. 873ac3.
1	801de3. 975dc6.
2	963da2. 963db2.
3	162dc1. 845be6.
4	
5	062be1. 665bd3. 975cb5.
6	
7	
8	078ea1. 165cd4. 078ab6.
9	
20	
1	873ae6.
2	776ca2.
3	030ba.
4	088dc5.
5	
6	143ad1. 460be.3 460ed6.
7	
8	
9	

30	
1	
2	
3	776cb3.
4	111ed1. 897ba6. 897ae4. 208ba5. 208be5.
5	
6	
7	335ec6.
8	
9	205ac1. 205da4. 953bc4. 953ec4. 953db5. 205bd6.
40	170bc6.
1	161ec2. 161ea3.
2	
3	589ab3.
4	
5	
6	
7	273ec1. 273ae2. 360ec4. 078bd4. 078ed4. 959ed5. 959ad5. 273ad6. 273be2.
8	335cd3.
9	173bd1. 173ca5. 173ce5.
50	
1	974ed2. 974ec3.
2	235bc1. 962da3. 962ca6.
3	
4	
5	

II B2b2

Determining the reduction numbers.

Difference	Position	Group I	Group II	reduction number	for column
39205	1 a c	30625	01420	00000	1
	4 d a	22133	93938	18592	4
	6 b d	59477	20272	81258	6
18078	1 e a	48693	30625	00000	1
	6 a b	67445	59477	81258	6
26460	3 b e	61717	65357	66173	3
	6 e d	46632	20272	81258	6
10813	3 a c	04296	96483	66173	3
	2 c d	28484	18671	42985	2
39950	4 b c	69141	30298	18592	4
	5 d b	84909	55056	93734	5
49173	1 b d	53655	14582	00000	1
	5 c a	60921	21858	93736	5
41161	2 e c	69545	28484	42985	2
	3 e a	65357	04296	66173	3
47273	1 e c	48693	01420	00000	1
	2 a e	06718	69545	42985	2
	6 a d	67445	20272	81258	6
57976	2 e d	69545	18671	42985	2
	3 e c	45357	94483	66173	3
2962	3 d a	56158	04296	66173	3
	6 c a	19307	67665	03924	6

TOP SECRET

Doc ID: 6592460

Difference Catalogue

00	197:	48780 48693						
1								
2	361:	14582 12221						
3	109:	53655 50556						
4								
5								
10	873:	60369 50556						
1	801:	12221 01420	975:	01420 90555				
2	963:	50556 48693	875:	50556 48780				
3	845:	30625 27880	162:	14582 01420	308:	27880 14582		
4								
5	062:	53655 48693	975:	53655 48780	669:	27880 12221		
6								
7	714:	60369 53655	374:	77633 60369				
8	078:	48693 30625	165:	48780 30625				
9								
20	931:	50556 30625						
1	813:	68693 27880	900:	68780 27880				
2	776:	60369 48693	689:	60369 48780	776:	12221 50555		
3	030:	53655 30625	922:	90555 77633				
4	088:	77633 53655	037:	14582 90555				
5								
6	143:	30625 16582	460:	27880 01420				
7	187:	77633 50556						
8	404:	30625 12221						
9	205:	30625 01420						

II B 2 b - 3 (a)

30	744:	60365	296:	90555							
		30625		60369							
1											
2											
3	776:	50556									
4		22880									
4	897:	01420	111:	48693	208:	48780					
		77633		14582	1458	14582					
5											
6	875:	53655	472:	48693	569:	48780					
		27880		12221		12221					
7	335:	27880									
		90555									
8											
9	205:	30625	040:	77633	953:	77633					
		01420		48693		48780					
40	170:	30625	009:	90555							
		90555		50556							
1	434:	53655	161:	01420							
		12221		60365							
2											
3	589:	60369									
		23880									
4											
5	698:	12221									
		77633									
6	074:	50556									
		14582									
7	078:	77633	900:	90555	273:	68693	360:	68280	959:	14582	
		30625		53655		07420		01420		77633	
8	335:	50556									
		12221									
9	173:	53655									
		14582									
50	257:	27880									
		77633									
1	974:	01420									
		50556									
2	235:	53655	962:	90555	962:	12221	875:	90555			
		07420		48693		60369		48780			
3											
4	223:	14582									
		60369									
5											

IIB
2b3b

Doc ID: 6592460

Study of reduction numbers

Reduction number in column

1	00000
2	42985
3	66173
4	18592
5	93734
6	81258
1	00000

Original reencipherment number

3 5 4 2 7 9

Difference of reduction numbers

1 + 2	42985	
2 + 3	24298	
3 + 4	52429	
4 + 5	85242	= 4 2 9 8 5 2 4
5 + 6	98524	
6 + 1	29852	

Possible reduction numbers derived according to the complementary value of the intermediate difference 6 8 1 2 5 8:

0 8 9 1 6 4, 1 9 0 2 7 5, 2 0 1 3 8 6, 3 1 2 4 9 7, 4 2 3 5 0 8,

5 3 4 6 1 9, 6 4 5 7 2 0, 7 5 6 8 3 1, 8 6 7 9 4 2, 9 7 8 0 5 3.

IIB 2b3c

Doc ID: 6592460

Reduced cipher text

Reduction number	0 8 9 1 6 4	0 8 9 1 6 4	0 8 9 1 6 4	0 8 9 1 6 4	0 8 9 1 6 4	0 8 9 1 6 4
Column	1	2	3	4	5	6
Reduced cipher text	3 8 5 3 1	4 6 5 0 9	6 8 2 7 5	0 9 3 3 6	1 2 4 9 8	4 6 5 0 9
	5 1 5 6 1	4 6 5 0 9	2 5 7 9 6	5 5 5 4 9	4 6 6 9 6	3 8 5 3 1
	0 9 3 3 6	0 0 1 5 0	1 4 5 3 5	5 4 1 8 8	4 4 2 9 5	7 9 6 1 9
	1 2 4 9 8	5 8 4 6 2	1 0 1 3 7	3 8 5 3 1	7 5 5 4 9	0 9 3 3 6
	4 6 5 0 9	0 9 3 3 6	0 9 3 3 6	7 5 5 4 9	1 2 4 9 8	2 5 7 9 6

Reduction number	7 5 6 8 3 1	7 5 6 8 3 1	7 5 6 8 3 1	7 5 6 8 3 1	7 5 6 8 3 1	7 5 6 8 3 1
	1	2	3	4	5	6
Reduced text	0 5 2 0 8	1 3 2 7 6	3 5 9 4 2	7 6 0 0 3	8 9 1 6 5	1 3 2 7 6
	2 8 2 3 8	1 3 2 7 6	9 2 4 6 3	4 2 2 1 6	1 3 3 6 3	0 5 2 0 8
	7 6 0 0 3	3 5 9 4 2	2 5 1 3 9	1 3 3 6 3	2 8 2 3 8	6 5 1 3 8
	8 9 1 6 5	2 5 1 3 9	8 7 8 0 4	0 5 2 0 8	4 2 2 1 6	7 6 0 0 3
	1 3 2 7 6	7 6 0 0 3	7 6 0 0 3	4 2 2 1 6	8 9 1 6 5	9 2 4 6 3

II B2b4

Doc ID: 6592460

Key number = SZ Reencipherment number ÜZ (= additive)

1) SZ 13450
" ÜZ 47954 16495 70342 73769 00359 03849
31232 43556 78013 58148 39521 .....

2) SZ 134500
" ÜZ 47950 41645 45709 99279 88196 76905
33595 86844 34287 78605 45465 99900 .....

3) SZ 134501
" ÜZ 47951 51646 66700 22370 24507 26957
98542 67396 83025 41327 95459 6....

4) SZ 17340 20419 03380 6
" ÜZ 80742 24509 36186 48716 46959 29794
02587 00544 11663 42735 70598 52729
76908 27547 37991 63598 09291 00680 ....

5) SZ 17340 20419 03380 61
" ÜZ 80742 24509 36186 79871 64695 92979
43675 87005 44116 63793 23570 59852
72906 25582 75473 79919 68703 09491
00680 0.....

6) SZ 17340 20419 03380 612
" ÜZ 80742 24509 36186 73087 16469 59297
94303 85870 05441 16637 33135 70598
52723 00644 68275 47379 91906 08040
92910 06800 9.....

TOP SECRET

Doc ID: 6592460

7) SZ 5 1 9 3 6 7 0 3 7

ÜZ 6 0 2 9 3 7 3 0 3 6 2 1 2 0 0 3 3 9 8 3 3 2 0 3 6 2 7 1 6 5
2 3 9 8 9 8 7 1 7 5 2 7 7 7 5 8 8 2 7 9 4 4 2 3 6 0 9 6 3 8
6 5 9 6 9 5 9 1 4 1 4 5 5 4 4 0 5 5 5 9 0 3 8 4 . . . . . .

---

8) SZ 6 3 2 8 5 4 2 6

" ÜZ 9 5 0 3 9 6 8 5 4 5 3 2 5 4 3 9 9 8 5 7 9 7 2 8 7 3 2 6 6 9
0 5 0 5 8 2 5 9 5 5 5 3 0 7 4 4 0 0 8 3 7 1 8 4 0 8 . . . .

---

9) SZ 5 1 9 3 6 7 0 3 7 6 3 2 8 5 4 2 6

ÜZ 6 0 2 9 3 7 3 0 3 9 5 0 3 9 6 8 2 6 2 1 2 0 0 3 3 2 4 5 3 2
5 4 0 8 8 3 3 2 0 3 6 5 6 9 8 5 7 9 4 8 6 1 6 5 2 3 9 1 1 5
7 3 2 6 3 2 4 7 7 1 7 5 2 0 2 6 2 0 5 8 9 5 6 1 4 8 8 2 7 2
2 8 8 2 5 3 7 4 1 7 5 2 6 0 9 9 4 0 6 0 7 8 0 1 5 8 2 7 8 6
9 8 3 4 6 6 7 5 8 1 6 3 0 9 5 4 5 7 1 7 0 2 3 2 3 . . . . .

---

10 a) SZ 3 9 6 2 4 0 2

" ÜZ 2 5 8 6 4 2 4 7 3 4 0 6 6 1 0 7 4 6 2 7 1 7 1 0 8 9 8 8 8 1
8 7 7 6 6 9 9 5 4 3 2 5 8 4 . . . .

b) " ÜZ 2 5 8 6 4 2 X 7 3 4 0 6 9 0 7 4 6 5 9 7 1 0 1 4 6 8 1 1 5 0 4
9 2 6 5 4 3 1 8 1 . . . . . .

c) " ÜZ 2 5 8 6 4 2 5 7 3 4 0 6 7 2 0 7 4 6 3 9 2 7 1 0 9 2 1 9 8 1
9 1 3 0 7 9 0 0 4 3 7 6

---

11) SZ 3 6 7 2 X 3 5 9

" ÜZ 9 3 5 X X 8 4 8 2 8 X X X 2 2 0 0 X X X X 4 2 0 X X X X X 6
2 X X X X X X 8 X X X X X X X X X

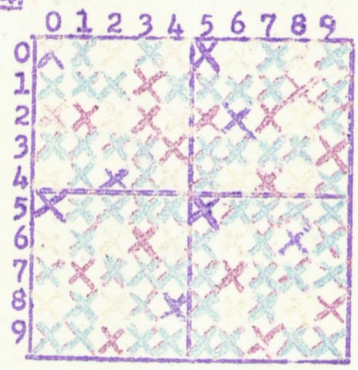
II B 2 e - 1 b

IIB
2elb

Doc ID: 6592460

Length of Russian additive with 2-digit key:

S Z	" U Z	Length
0 0	0 0	1
0 1	1 2 3 5 8 3 1 4 5 3 4 3 7 0 7 7 4 1 5 6 1 7 8 5 3 8 1 9 0 9 9 8 7 5 2 7 9 6 5 1 6 7 3 0 3 3 6 9 5 4 9 3 2 5 7 2 9 1 0 1	60
0 4	4 8 2 0 2 2 4 6 0 6 6 2 8 0 8 8 6 4 0 4	20
0 5	5 0 5	3
1 3	4 7 1 8 9 7 6 3 9 2 1 3	12
4 2	6 8 4 2	4
		100



Length of Russian additive with 3-digit key:

		Length
0 0 0	0 0 0	1
0 0 1	0 1 1 1 2 2 3 4 5 7 9 2 6 1 8 7 9 5 6 4 1 0 5 1 5 6 6 1 2 7 3 9 0 2 9 2 1 1 3 2 4 5 6 9 1 5 0 6 5 6 1 1 7 2 8 9 0 7 9 7 6 6 3 2 9 5 1 4 6 5 0 1 5 1 6 6 7 2 3 9 5 2 4 7 6 1 3 7 4 0 1 4 1 5 5 6 0 1 6 1 7 7 8 4 5 2 9 7 1 6 8 7 4 5 1 9 6 0 5 6 5 1 1 6 2 7 8 9 5 7 4 2 1 6 3 7 9 0 6 9 6 5 5 1 0 6 1 6 7 7 3 4 0 7 4 7 1 1 8 2 9 0 1 9 1 0 0 1	168
0 0 2	0 2 2 2 4 4 6 8 0 4 8 4 2 2 6 4 8 0 2 8 2 0 0 2	24
0 0 3	0 3 3 3 6 6 9 2 5 1 7 6 8 3 4 1 7 5 8 2 3 0 5 3 5 8 8 3 6 1 9 7 0 6 7 6 3 3 9 6 2 5 8 7 3 5 0 8 5 8 3 3 1 6 4 7 0 1 7 1 8 8 9 6 7 5 3 2 8 5 0 3 5 3 8 8 1 6 9 7 5 6 2 1 8 3 9 1 2 0 3 2 3 5 5 8 0 3 8 3 1 1 4 2 5 6 7 1 3 8 4 1 2 5 3 7 8 0 5 8 5 3 3 8 6 1 4 7 5 1 2 6 3 8 9 1 7 0 8 7 8 5 5 3 0 8 3 8 1 1 9 2 0 1 2 1 3 3 4 6 7 0 3 7 3 0 0 3	168
0 0 4	0 4 4 4 8 8 2 6 0 8 6 8 4 4 2 8 6 0 4 6 4 0 0 4	24
0 0 5	0 5 5 5 0 0 5	7
0 0 6	0 6 6 6 2 2 8 4 0 2 4 2 6 6 8 2 4 0 6 4 6 0 0 6	24
0 0 7	0 7 7 7 4 4 1 8 5 9 3 4 2 7 6 3 3 5 2 8 7 0 5 7 5 2 2 7 4 9 1 3 0 4 3 4 7 7 1 4 8 5 2 3 7 5 0 2 5 2 7 7 9 4 6 3 0 9 3 9 2 2 1 4 3 5 7 8 2 5 0 7 5 7 2 2 9 4 1 3 5 4 8 9 2 7 1 9 8 0 7 8 7 5 5 2 0 7 2 7 9 9 6 8 5 4 3 9 7 2 6 9 8 5 7 3 2 0 5 2 5 7 7 2 4 9 6 3 5 9 8 4 7 2 1 9 3 0 2 3 2 5 5 7 0 2 7 2 9 9 1 8 0 9 8 9 7 7 6 4 3 0 7 3 7 0 0 7	168
0 0 8	0 8 8 8 6 6 4 2 0 6 2 6 8 8 4 6 2 0 8 2 8 0 0 8	24
	carry forward	608

TOP SECRET

Doc ID: 6592460

TOP SECRET

brought forward 608

009 0 9 9 9 8 8 7 6 5 3 1 8 4 9 2 3 1 5 4 6 9 0 5 9 5 4 4 9 8 3
7 1 0 8 1 8 9 9 7 8 6 5 4 1 9 5 0 4 5 4 9 9 3 8 2 1 0 3 1 3
4 4 7 8 1 5 3 6 4 5 0 9 5 9 4 4 3 8 7 1 5 8 6 3 4 9 7 3 6 0
9 6 9 5 5 4 0 3 4 9 3 3 2 6 5 8 1 3 9 4 2 3 6 5 9 1 4 0 5 4
5 9 9 4 8 3 2 1 5 3 6 8 9 4 7 3 1 0 4 1 4 5 5 9 0 4 9 4 3 3
7 6 0 3 6 3 9 9 2 8 1 0 9 1 9 0 0 9 / 168

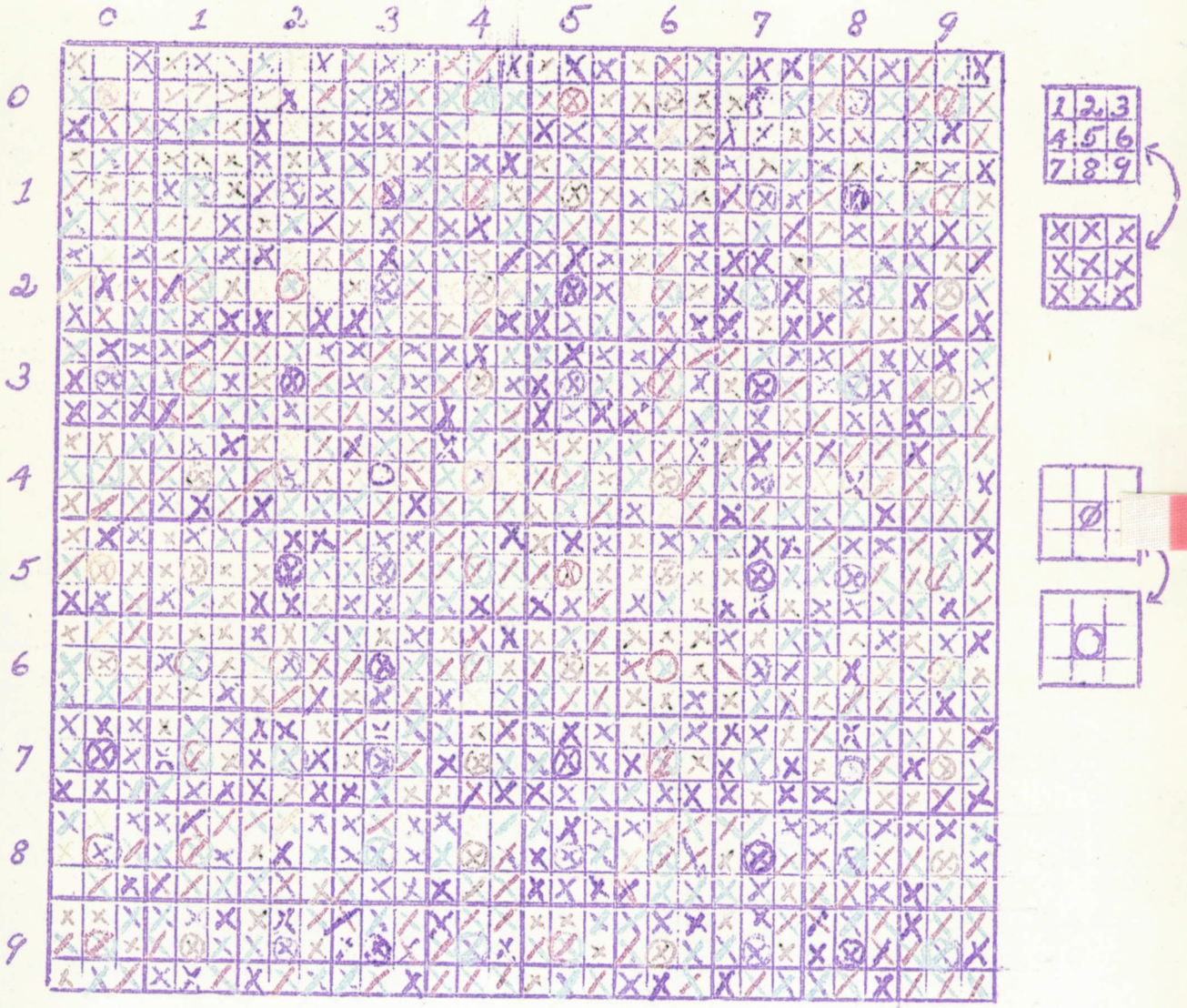
013 1 4 4 5 8 9 3 7 2 0 9 2 9 1 1 0 2 1 2 3 3 5 6 8 1 4 9 5 3 4
8 7 2 5 9 7 4 6 1 0 7 1 7 8 8 5 6 3 1 9 4 0 3 4 3 7 7 0 4 7
4 1 1 5 2 6 7 8 3 5 1 8 6 9 4 5 3 9 8 2 7 0 9 7 9 6 6 5 2 1
7 3 8 0 1 8 1 9 9 0 8 9 8 7 7 5 4 2 9 6 1 5 7 6 2 3 8 5 1 3
6 4 9 0 3 9 3 2 2 5 4 7 9 1 6 0 7 6 7 3 3 0 6 3 6 9 9 5 8 4
3 2 7 5 9 2 4 1 6 5 7 1 2 8 3 0 1 3 \ 168

026 2 8 8 0 6 8 6 4 4 0 8 4 8 2 2 0 4 2 4 6 6 0 2 6 / 24

124 3 6 7 9 3 6 2 9 8 1 7 9 8 6 7 4 3 1 7 4 8 1 2 9 3 1 2 4 / 28

248 6 2 4 8 / 4

1000



II B 2 e - 2 b

TOP SECRET

Doc ID: 6592460

3. Additive sequences for codes with groups of varying length.

Überschlüsselungszahlen für wechselstellige Codes

Since, when using additive, the danger lies in the fact that when the same additive is used several times the enciphered code group can be matched in columns and differenced, it is well to use the additive sequence in connection with codes having groups of different lengths. This prevents differencing by columns the remainder of the text on the basis of single parallel passages because the varying length of the code groups does not permit dividing up the rest of the cipher tex t by groups. Hence if an additive sequence of adequate length, e.g. in the form of an additive book, is used in connection with a code which has groups of different lengths, then such an additive may be used for some time without hesitation if it is certain that the indicators will not allow the cryptanalyst to deduce the starting points for the additive.

4. Additive in the substitution table system.

Die Überschlüsselungszahl im Tauschtafelverfahren.

Insofar as the additive sequence is to be used more than once there is another possibility present in the combination of the additive sequence and the substitution table. This combination represents a very essential improvement, insofar as solution by forming differences is out of the question even though the same additive is used a number of times. Since this system has first been used in France it is also termed the French additive system.

As substitution table, it is well to use a square with 9 cells, i.e. 3 rows and 3 columns. The digits 0 to 9 are entered in the square in random order leaving one digit outside the table to be used as a null. Such a table is shown at the top of sheet 1 of Appendix II B 4. Its use is as follows:

1.) If the code value to be enciphered and the additive value are both contained in the square, then we take as cipher value that digit which with the two given digits forms a row, a column or a diagonal. The square is to be extended in all directions correspondingly.

2.) If the digit of the additive and the digit of the code coincide, then the null is taken as cipher value.

3.) If the digit of the additive or the digit of the code coincides with the null then the non-coinciding value is taken for the cipher.

On sheet 2, three different texts have been enciphered by this system using the same additive sequence. The resulting message text corresponds outwardly to one which might have originated by using additive. Genuine parallel passages are possible in both cases only at the same point in the additive because like code groups at different points in the additive cannot appear as parallel passages.

For instance, although columns I and V each contain the two code groups 32750 and 16278, the corresponding cipher groups 57404 and 60337 or 16055 and 32876 no longer give any suggestion that like code groups are involved because differencing does not work.

Since the unauthorized decrypter has to rely solely on repetitions in the cipher text, the same additive sequence may be used with the same substitution table just as long as the repeats, whether within the columns or between the columns, give no clues for decryption. This means, however, that even with heavy traffic all messages for one day or even longer might be enciphered with the same material. Even assuming that the basic code is known, there would still be absolute security. Since the superencipherment consists of two parts of equal value, namely the additive and the substitution table, the loss or compromise of one of these factors would not necessarily compromise the day's traffic.

Consequently the combination of code, additive sequence and substitution table affords extraordinary security.

We have now covered all essentials of superencipherments and combined systems. Other combinations and other superencipherments are conceivable, to be sure, but it is quite certain that new points of view would appear which have not already been touched on.

TOP SECRET

Substitution table

6	0	4
2	5	8
9	7	1

Consists of one null (red) and nine single digit values which are arranged at random in a 3 x 3 square. Its effect corresponds to that of the following substitution table:

	0	1	2	3	4	5	6	7	8	9
0	3	2	1	0	6	7	4	5	9	8
1	2	3	0	1	8	6	5	9	4	7
2	1	0	3	2	7	8	9	4	5	6
3	0	1	2	3	4	5	6	7	8	9
4	6	8	7	4	3	9	0	2	1	5
5	7	6	8	5	9	3	1	0	2	4
6	4	5	9	6	0	1	3	8	7	2
7	5	9	4	7	2	0	8	3	6	1
8	9	4	5	8	1	2	7	6	3	0
9	8	7	6	9	5	4	2	1	0	3

II B41

The substitution table contains, once the null is determined:

28 constant substitution values, and

72 variable substitution values, which can be reduced to 12 different basic equations (if, for instance, 01 = 2, then 10 = 2, 02 = 1, 20 = 1, 12 = 0, 21 = 0).

It yields $\frac{10!}{9}$ possibilities.

TOP SECRET

Doc ID: 6592460

	I					II					III					IV					V					VI				
	0										1										2									
	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9
Encipherment sequence	5	4	2	7	6	0	3	4	3	1	3	2	0	5	4	6	3	8	2	4	1	9	5	3	7	4	5	9	6	2
Code text A	3	2	7	5	0	0	2	4	8	6	5	9	6	7	0	6	8	3	0	6	3	2	7	5	0	1	9	5	0	2
Cipher text A	5	7	4	0	4	3	2	3	8	5	5	6	4	0	6	3	8	8	1	0	1	6	0	5	5	8	4	4	4	9
Code text B	1	6	2	7	8	0	2	4	8	6	3	2	7	5	0	1	9	5	0	2	1	6	2	7	8	2	2	5	8	1
Cipher text B	6	0	3	3	7	3	2	3	8	5	3	3	5	3	6	5	9	2	1	7	3	2	8	7	6	7	8	4	7	0
Code text C	1	5	4	2	9	3	2	7	5	0	2	8	9	1	6	8	7	6	4	2	3	2	7	3	5	1	9	5	0	2
Cipher text C	6	9	7	4	2	0	2	2	5	2	2	5	8	6	0	7	7	7	7	7	1	6	0	3	0	8	4	4	4	3

Cipher	0 =	03	12	21	30	46	57	64	75	89	98
"	1 =	02	13	20	31	48	56	65	79	84	97
"	2 =	01	10	23	32	47	58	69	74	85	96
"	3 =	00	11	22	33	44	55	66	77	88	99
"	4 =	06	18	27	34	43	59	60	72	81	95
"	5 =	07	16	28	35	49	53	61	70	82	94
"	6 =	04	15	29	36	40	51	63	78	87	92
"	7 =	05	19	24	37	42	50	68	73	86	91
"	8 =	09	14	25	38	41	52	67	76	83	90
"	9 =	08	17	26	39	45	54	62	71	80	93

II B42

TOP SECRET

Doc ID: 6592463

~~TOP SECRET~~

SECURITY INFORMATION

ARMED FORCES SECURITY AGENCY

DF-240 Parts III and IV

22/52/~~TOPSEC~~/AFSA-14

Copy No. 35

From: AFSA-14

To: ARCHIVES, AFSA-252H

/THIS DOCUMENT CONTAINS INFORMATION AFFECTING THE NATIONAL DEFENSE OF THE UNITED STATES WITHIN THE MEANING OF THE ESPIONAGE LAWS, TITLE 18, U.S.C., SECTIONS 793 AND 794. SEE ALSO PUBLIC LAW 513, 81ST CONGRESS, SECOND SESSION. ITS TRANSMISSION OR THE REVELATION OF ITS CONTENTS IN ANY MANNER TO AN UNAUTHORIZED PERSON IS PROHIBITED BY LAW./

Approved for Release by NSA on 09-12-2017, FOIA Case #67677

~~TOP SECRET~~

Doc ID: 6592463

DF 240 Parts III and IV 22/52/~~TOPSEC~~/AFSA-14

CHARACTERISTICS, ANALYSIS AND SECURITY

OF CRYPTOGRAPHIC SYSTEMS

1. Attached is an Armed Forces Security Agency translation of Parts III and IV of a treatise on cryptology prepared by Dr. Bruno KRÖGER, formerly with the Forschungsamt. German title: Systematik, Analyse und Sicherheit der Geheimschriften.

2. This treatise purports to cover in detail the work given in the course at the Forschungsamt. Since the methods described here are not essentially different from those used by AFSA, the primary value will be found in the picture it gives of the approach to these problems of another major cryptologic unit.

Translated : R.W.P. 35 copies

March 1952 45 pages

Distribution: Normal

Doc ID: 6592463

TABLE OF CONTENTS

		Page
III.	Cipher Machines	5
	Chiffriermaschinen	
A.	German Cipher Machines	6
	Deutsche Chiffriermaschinen	
1.	Enigma Cipher Machines	6
	Enigma-Chiffriermaschinen	
a)	Type K	6
	Typ K (See DF 240 B)	
b)	Type G	16
	Typ G	
c)	Army Enigma	17
	Heeres-Enigma	
	Appendix III A 1 a	18 to 26
2.	The Siemens Cipher Teleprinters	27
	Siemens-Geheimfernschreibmaschinen	
3.	The Army Supplemental Device (SZ 40, SZ 42)	31
	Heereszusatzgerät	
B.	Non-German Cipher Machines	32
	Nichtdeutsche Chiffriermaschinen	
1.	Japanese Cipher Machine	32
	Japanische Chiffriermaschine	
2.	Hagelin Cipher Machines	34
	Hagelin-Chiffriermaschinen	
3.	Russian Multi-channel Radio Cipher Machine	37
	Russische Mehrkabel-Funkmaschine	
4.	English Cipher Machine	39
	Englische Chiffriermaschine	
C.	Significance of Indicator Groups With Machine Systems	41
	Kenngruppenbedeutung bei Maschinen-Verfahren	

Doc ID: 6592463

Page

IV. General observations 43

Allgemeine Bemerkungen

A. Characteristics of Cryptographic Systems

Systematik der Geheimschriften

B. Analysis of Cryptographic Systems

Analyse von Geheimschriften

C. Security of Cryptographic Systems

Sicherheit von Geheimschriften

PART III

CIPHER MACHINES

(CHIFFRIERMASCHINEN)

That cipher machines are not taken up until the treatment of all substitution and transposition systems and of all combined and super-enciphered systems has been concluded is due to the fact that cipher machines in their characteristics do not differ from the manual systems. The reason for treating them in a separate part is that a discussion of the technical peculiarities of each cipher machine is necessary before we attempt to apply the basic knowledge already gained from the manual systems.

It is a common characteristic of all the cipher machines treated in the following pages that they must all be regarded as polyalphabetic substitutions since, when enciphering continuous plain text, each element is enciphered with a different alphabet. These alphabets always have a definite connection with one another which can be explained by the construction of the machine. Moreover the sequence in which these alphabets are used is to be regarded as the expression of a systematic character inherent in the construction of the machine.

Therefore the only thing that is new in the study of cipher machines may be the inner connection existing between the individual cipher alphabets insofar as a parallel to their structure and sequence may not always be found among the manual systems.

Since the different cipher machines that have been developed in different countries have no essential relation to one another, the order in which they are taken up can be an arbitrary one.

Doc ID: 6592463

SECTION A

GERMAN CIPHER MACHINES

(DEUTSCHE CHIFFRIERMASCHINEN)

Since the writer's professional concern with the security of German cipher machines was limited to cases where these machines were also used by foreign countries, the treatment of certain German machines will have to be limited to basic considerations because technical details are not always known to him.

1. The Enigma cipher machine.

Die Enigma-Chiffriermaschine

Three different types of Enigma machines were developed. The basic type, from which the other two were derived later, is the Enigma cipher machine Type K.

The construction and functioning of Enigma Type K is assumed to be known. It has been represented schematically by a paper device shown in Appendix III A 1 a, sheet 1.* Using this paper device shy cipher text can be produced just as well as with the machine, provided the wheel wiring corresponds.

In Appendix III A1 a, sheet 1, the column of letters at the right side corresponds to a fixed disk in the original machine which lies at the right of the right hand movable wheel. This disk in the machine is connected both with the keyboard and with the light bulbs under the letter panel in the sequence of this column, hence in what follows this column is designated as the endplate sequence.

The paper strips I, II and III represent the wheels which may be placed in positions A, B and C according to the wheel order selected. The outer number sequences from 1 to 26 at the right and left on each strip correspond to the 26 points of entry and exit on each wheel.

* This study of the Enigma Type K was submitted earlier as a sample of what Kröger planned to do and was issued as DF 240 B.

We designate as point 1 that point of each wheel at which the letter rings are set. The inner number sequences indicate the wiring within a wheel; the numbers of these inner sequences indicate the point on the opposite side of the wheel to which the point of entry or exit is connected. The two columns of numbers standing on the left side of the paper device correspond to the reversing wheel or mirror in a definite position and with a given wiring.

The sequences of letters in the center of the strips represent the setting rings on the wheels in a particular setting. The lines between the letters m and n on wheel I, f and g on wheel II, y and z on wheel III are to indicate the notches on the setting ring which the stepping levers (indicated by an arrow on the paper device) engage when the wheel reaches the appropriate point and which thus cause the stepping of the middle or left wheel. The hatched squares on the lowest row (on a level with q of the input alphabet) are intended to represent the windows in which the window setting of the wheels is visible.

With this paper device, using an arbitrary wheel order I, III, II, an internal ring setting v on wheel I, l on wheel II and h on wheel III and with the outer window setting n c f for the three wheels, all cipher values for the plain letters of the endplate sequence have been developed in 26 successive positions of the right hand wheel and these are shown in Appendix III A 1 a, sheet 2. The first twenty-one of the resulting alphabets have been separated from the last five by a vertical stroke because at this point the middle wheel made a step. Therefore the complex: reversing wheel, wheel I and wheel III which forms a reversing mirror, changed at this point.

The following description of the regularities of the cipher text of the Enigma Type K is based on the fundamental idea that the reversing wheel, left wheel and middle wheel form a constant during the encipherment of 26 letters which lie between the steps of the middle wheel. The encipherment of 26 successive letters is therefore based solely on:

1. The wheel wiring of the right wheel, and

2. of the mirror complex composed of the reversing wheel, the left wheel and the middle wheel.

The purpose of the following discussion is therefore to develop the cipher text following Appendix III A 1 a, sheet 2, in such fashion that the regularities inherent in the wiring of the right wheel and in the reversing mirror become recognizable.

For this purpose the alphabets in Appendix III A 1 a, sheet 2, have been converted into numerical values on sheet 3 in such manner that the letters q to m have been converted into the input values 21 to 20 valid with the initial setting f of the right hand wheel.

In Appendix III A 1 a, sheet 4, 1 has been added to the numerical values of the second alphabet (i.e., of the second vertical column of numbers) shown on sheet 3, 2 to those of alphabet 3, 3 to those of alphabet 4, etc., thus transforming all cipher letters of Appendix III A 1 a, sheet 1, into the input values of this wheel for the momentary position of the right wheel. This transformation causes the substitution values of III A 1 a, sheet 1, to be reduced to a uniform denominator independent of the movement of the right wheel.

On sheet 4 the numerical substitution values standing in the diagonals running down from left to right have been formed by the same wheel wiring leading from the endplate alphabet to the reversing mirror.

These diagonals have been taken out and arranged horizontally on sheet 5. Closer examination shows that these sequences are similar in pattern, as is revealed by a comparison of diagonal 7 and diagonal 6. Here the isomorphic relationship of each row with any other row is revealed, displaced in each case by one value to the right. The values found in these diagonals always have the same wheel wiring in the path from the endplate alphabet to the reversing wheel (lying between the middle and right hand wheel) and therefore

use successively all mirror wirings of the reversing complex corresponding to the progress of the right wheel. The isomorphism between the diagonals is therefore merely a reflection of the reversing wheel valid for the right hand wheel.

To explain this we have shown in Sheet 6:

1. A reversing mirror valid for the right wheel with the window setting n c f as it is formed by the complex: reversing wheel, wheel I and wheel III;
2. The same reversing complex expressed in the difference values between the contacts. (Schaltpunkten);
3. Two different diagonals from sheet 5 at the level corresponding to the reversing complex.

The isomorphic relationship of the diagonals to the reversing complex expressed in differences thus becomes obvious.

Now if all the diagonals are arranged according to their isomorphic relationship to the reversing complex, as has been done on sheet 7 and sheet 8 (in this case with the displacement of 1), it appears from sheet 8 that with this arrangement all the vertical columns of numbers as well as the number sequence of the diagonals are no more than a reflection of the wheel wiring of the right wheel as contained in the inner left column of wheel II in Appendix III A 1 a, sheet 1.

With this we have shown that by converting the plain and cipher letters into corresponding numerical values of the endplate sequence the wheel wiring of Enigma Type K can be reconstructed. This possibility of reconstruction depends on the systematic derivation of 26 successive alphabets by turning one wheel while the other wheels remain still.

On the basis of the regularities just disclosed we find the following possibilities for solving Enigma Type K:

Possibility A.

We assume as known three successive alphabets which have been obtained, let us say, by solving several messages in the same key or in some other fashion.

These alphabets are converted in the manner indicated above into numerical values and written out on strips corresponding to the rows of Appendix III A 1 a, Sheet 8. We shall use as an example the first three alphabets from the previous example after the stepping of the middle wheel, i.e., alphabets 16 to 18 on Sheet 4 as they appear on Sheet 8. This gives us the following strips:

1	20	13	24	10	15	4	5	19	13	6	25
2	8	9	8	11	18	23	4	20	1	3	6
3	9	20	14	12	22	15	13	21	7	8	22
4	6	10	11	13	19	1	12	22	12	18	21
5	14	25	10	14	5	24	3	23	26	11	7
6	4	19	20	15	10	12	16	24	16	14	1
7	21	17	23	16	24	26	15	25	17	5	19
8	2	21	2	17	25	7	18	26	23	16	9
9	3	2	26	18	11	22	17	27			

Starting with any strip, the other strips are matched with it successively until it can be deduced from the juxtaposition whether the selected strip or wheel wire sequence is correct or not. First we shall assume that initial strip 17 is followed by strip 18.

17 25 7 18

18 11 22 18

The columns 7 11 and 18 22 resulting from this superimposition signify, according to the regularities set forth on page 8 that with an assumed wiring sequence (Walzenschaltungsfolge) 17 18 we get also the sequences 7 11 and 18 22. If the strips corresponding to these sequences are superimposed and inferences are drawn, we get the following.

1.) 7 21 17 13 18 11 22 17

11 18 23 4 22 12 18 21

Since this would give us the new sequence 23 23, which is impossible, we have proved that the assumed sequence 17 18 was false.

We next make the assumption that strip 17 is followed by strip 19. This yields the following:

1.)	17		25	7	18										
		19		13	6	25									
2.)	7		21	17	23			18		11	22	17			
		13		19	1	12			6		4	19	20		
3.)	23		25	11	7			22		12	18	21			
		1		20	13	24			4		6	10	11		
4.)	11		18	23	4			21		7	8	22			
		20		1	3	6			10		15	4	5		
5.)	4		6	10	11			8		2	21	2			
		3		9	20	14			15		10	12	16		
6.)	10		15	4	5			2		8	9	8			
		9		3	2	26			12		22	15	13		
7.)	5		14	25	10			9		3	2	26			
		2		8	9	8			22		12	18	21		
8.)	25		17	5	19			26		23	16	9			
		8		2	21	2			18		11	22	17		
9.)	19		13	6	25			16		24	26	15			
		21		7	8	22			11		18	23	4		
10.)	6		4	19	20			15		10	12	16			
		7		21	17	23			23		26	11	7		
11.)	20		1	3	6			12		22	15	13			
		17		25	7	18			26		23	16	9		
12.)	3		9	20	14			13		19	1	12			
		25		17	5	19			16		24	26	15		
13.)	14		5	24	3			1		20	13	24			
		5		14	25	10			24		16	14	1		
14.)	24		16	14	1										
		14		5	24	3									

From these fragments we get the entire wheel wiring of the right wheel as follows:

17 19 21 10 9 22 4 3 25 8 15 23 1 24 14 5 2 12
26 18 6 7 13 16 11 20 17.

This example likewise shows that a minimum of three alphabets is adequate for the recovery of the wheel wiring. (However, if the reversing complex for the alphabets concerned has two successive parallel wirings at the same interval, then a fourth alphabet will be necessary in order to recover the complete wiring sequence.

Otherwise we shall get several fragments which contain no contradictions, but it will be necessary to test out the correct combination with the cipher text). With the wiring of the right wheel thus obtained we can for the moment only produce a wheel which is equivalent in its effect, since from the wiring sequence itself the points on the left side of the wheel to which it is to be associated are not evident. Hence we have to make an arbitrary assumption which yields one of the 26 possible wheels which have the same effect. Which of the 26 represents the original wheel can only be determined after reconstructing the remaining wheels.

For reconstruction of the middle wheel it is necessary to have three alphabets at an interval of 26 which are used as in the above example. The requisite three alphabets at an interval of 26 can be picked out of the traffic fairly easily. Here the procedure is to associate to the cipher text an assumed plain text (frequent telegram beginnings or some word which may be expected to occur in the text because of the link or of contemporary events) so that for each possible juxtaposition of plain text with cipher text (with the already recovered wheel) mirror connections are produced which result from the 26 possible initial positions of the wheel and the input alphabet. If contradictions appear in the mirror connections, that means that the assumed word cannot stand at that particular point with the assumed initial wheel position. If no contradictions result, the mirror connections obtained are used to get new plain text letters to the right and left in the passage of cipher text. If these can be extended to yield reasonable text and if the extension confirmd the mirror connections already obtained, then the accuracy of the assumption is proved. After that it is merely a question of expanding the text beyond those points where the middle wheel steps and of continuing to expand the text on the basis of the newly obtained connections of the new mirror complex until some 60 to 80 letters of plain text are available with associated cipher text.

Then by recovering the input alphabet for the middle wheel it is possible to form three alphabets at an interval of 26 which will permit a reconstruction of a middle wheel having the same effect as the original.

The third wheel can be recovered in the same manner by using a cipher text where this third wheel is in the middle position.

From the equivalent wheels thus obtained it is possible to recover the original wheels if the window setting of three cipher texts which have been solved is known, provided each of the wheels I, II, and III occupies the right hand position in one of the messages. From the window setting and the stepping of the middle wheel it can be determined which of the three wheels corresponds to the original wheel I, II or III. The right side of the wheel is then brought up to the original values by adding some number between 0 and 25. With the aid of the solved text, the left sides are also brought into the original setting by turning the wiring sequence to that position where the different wheels function correctly together.

When the keys are sent in clear or are known, any message can be read by setting the inner and outer key as would be done at the receiving station.

If only the plain window setting is known while the inner wheel setting is not known but remains constant for a definite period of time, solution of one telegram by means of a crib is enough to enable reading all the other messages of that period.

On the other hand, if the inner and outer settings are not known, then for each individual message it will be necessary to force an entry by trying a probable word. This takes a lot of time when done by hand; it is quite possible to produce auxiliary machines working with electric relays by the aid of which a speedier break into almost every message becomes possible.

Possibility B: We assume as known a so-called compromised text, i.e., a cipher text which has been compromised because the plain text

has become known. This compromised text must have a length of 62 to 65 letters, depending on the position of the steps of the middle wheel. The substitution values obtained from the plain text and cipher text are transformed into numerical values by the method described on pages 8 and 10 and written out on strips. In contrast to the strips of 3-cell width used for the reconstruction of the wheel wiring under Possibility A, the strips used here are of a width corresponding to the length of the text and have only scattered substitution values on them. We now employ these strips very much as we did those described in the Possibility A, with the sole difference that in addition to an original assumption regarding the wiring sequence we have to make a 2nd, 3rd, 4th or even a 5th assumption before it is possible to determine whether the assumptions made were correct or not. This would work out somewhat as follows:

If the first assumption of a sequence 1 2 yields no clue regarding another resulting sequence, or if a resulting new sequence leads to no conclusion regarding the correctness of the first assumption, it is expanded by a second assumption of a wheel wiring sequence 1 2 3 or even 1 2 3 4; i.e., we keep making a new assumption until the possibility of this assumption is eliminated by resulting contradictions. The process is continued until by the elimination of the impossible wheel wiring sequences the correct sequence is found where no contradiction occurs.

If the original window settings for the compromised text employed are not known, this work is rendered more difficult by the fact that we have to guess the positions in the text where the middle wheel stepped. Hence we have to assume the step for all positions at an interval of 26 because superimposed substitution values on two strips only lead to correct deductions regarding other sequences when they have been produced with the same setting of the middle wheel.

To give some idea of the extent of this labor, it may be stated that the reconstruction of the first wheel by this method can be

accomplished by five or six workers in from one to six weeks, depending on whether one stumbles on the original sequence early or late in the process.

The reconstruction of the two remaining wheels can then be accomplished relatively quickly in the manner described under Possibility A.

Since the wheel wirings are soldered, no daily change in wiring is possible. From the standpoint of security it is necessary, therefore, to demand that this system be incapable of solution by the unauthorized cryptanalyst even when the system as such is known, i.e., in the present case when it must be assumed that the machine and wheel wiring are known. The Enigma Type K by no means satisfies any such security requirements, as is apparent from the preceding, because a single correctly guessed word leads to the solution of the message. Proper handling of the keys can at most make it necessary to solve each message individually but can never make solution of telegrams impossible. If special auxiliary devices are used for decipherment, no essential delay in reading can be assured. Even a frequent change of wheel wiring will not satisfy the security requirements. That we are not talking of exaggerated demands for security will be shown by the supplemental remarks in Part IV, Section C of this report.

The principle of encipherment by rotors, which is good in and of itself, would only yield adequate security if the machines were completely redesigned. The basic requirements for such redesign would be:

1. The regular wheel stepping must become very irregular and be capable of setting by some appropriate device.
2. The reversing combinations must be easily varied by appropriate devices.
3. The input alphabet must be capable of variation by plug connections between the keyboard and the input plate.
4. The reciprocal character of the alphabets generated must be done away with.

In any event there is no possibility of using the Enigma Type K in its present state so as to satisfy security requirements.

Of course there would be a possibility of reenciphering the cipher text by the machine or the plain text could be enciphered by another system and then reenciphered with the Enigma. However, this would never be satisfactory because encipherment and decipherment would take too much time and simple manual systems would afford greater security and faster work.

Enigma Type G

To make it impossible for the unauthorized cryptanalyst to follow the course of solution just described, the regular stepping of the wheel was abolished in the next type, the Enigma Type G. This was accomplished by providing the setting rings not merely with one notch but with a considerable number of notches distributed at irregular intervals on the ring. Since these notches cause the stepping of the middle and left hand wheel, this results in an irregular stepping of those wheels. Consequently the complex: middle wheel, left wheel and reversing wheel changes at short irregular intervals.

This means that the method of wheel recovery used for Type K is no longer useful.

On the other hand, the total period of the machine can be shortened, depending on the arrangement of the notches, so that with heavy use of a specific wheel-wiring and a specific wheel sequence it might be possible to reach a solution of the original columnar alphabets on the basis of parallel passages including digraphs and single cipher values for the most common plain values by lining up enough cipher texts.

This danger might have been countered easily by supplying a set of, let us say, ten wheels instead of the usual three. Three wheels would then be selected from among the ten and placed in the machine according to a frequently changing key. This would not merely result in considerably lengthening the total period of the machine but would at the same time have raised the number of sequences for the wheel positions from the former $3! = 6$ to $10! =$ over $3\frac{1}{2}$ million.

As a result, the difficulty in changing the wheel wirings and the sequence of the notches, which remain constant for each wheel in spite of their irregularity, would play a far less important role in respect to the resultant decrease in security.

It seems incomprehensible that the development in this essentially favorable direction was started but was broken off prematurely.

Army Enigma

In any case the Enigma most widely used in Germany, the Army Enigma cipher machine, gave up entirely the advantage of irregular stepping. Moreover it dispensed with the movable reversing wheel so that only three windows were provided for the external wheel setting.

Instead, the Army Enigma was improved to the extent that the previously fixed connections between the key-board and the fixed disk of the input alphabet were made pluggable, not at will, to be sure, but at least by pairs of letters. Thus if the key p was connected with input point x instead of with the input point p, key x was connected with input point p.

The resulting regularity in the plug connections, in connection with the reciprocal character of the machine led, in some way not known to me in detail, to a possibility of solution of a single message as soon as it contains more than 500 letters of continuous text provided the internal wheel wirings are assumed to be known. Essential for recognizing the existing plug connections is a count of the cipher text in a square 26 x 26 corresponding to the 26 positions of the wheels during one revolution and to the 26 cipher elements. This count showed along the diagonals a mirror like structure so that a heavy score in cell ib generally corresponds to a heavy score in the cell bi. The more heavily scored cells are a consequence of the plug connection and indicate which letters were substituted through the plug board. After solving the plug connections the rest of the solution may be accomplished by the same methods as were described for Enigma Type K.

Doc ID: 6592463

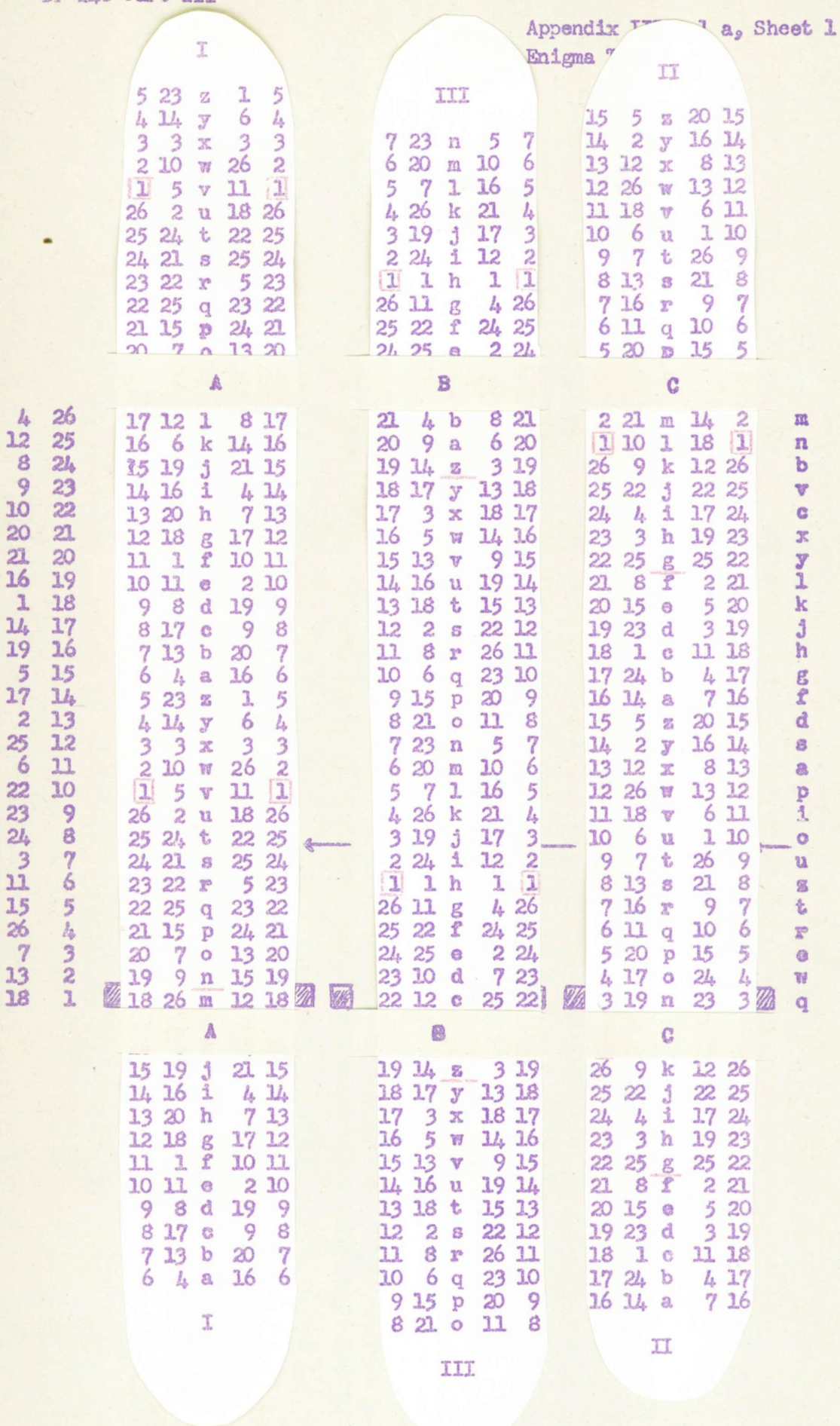
TOP SECRET

DF 240 Part III

Appendix [illegible] a, Sheet 1

Enigma [illegible]

App. III A1



TOP SECRET

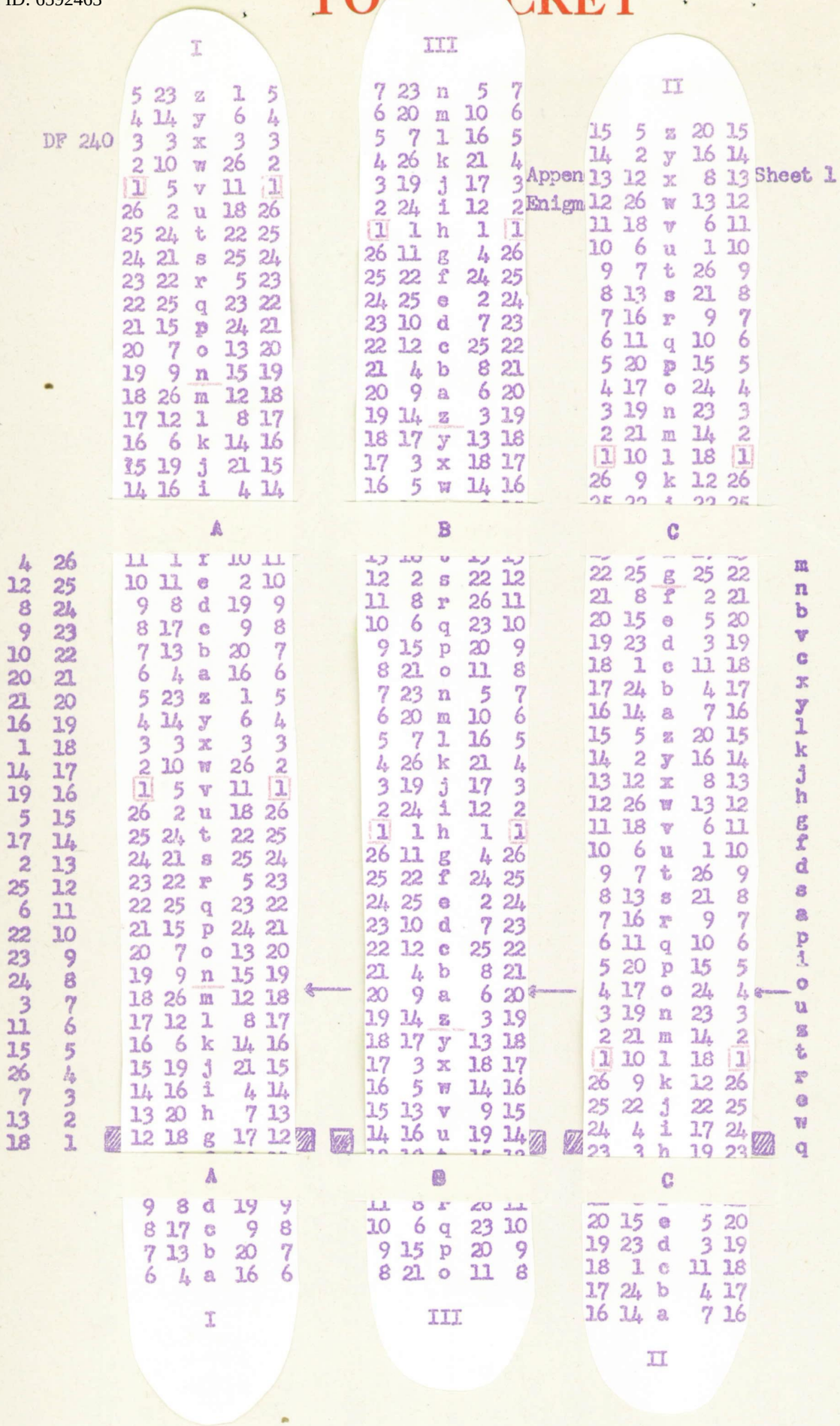
Doc ID: 6592463

TOP SECRET

DF 240

Appen Enigm

Sheet 1

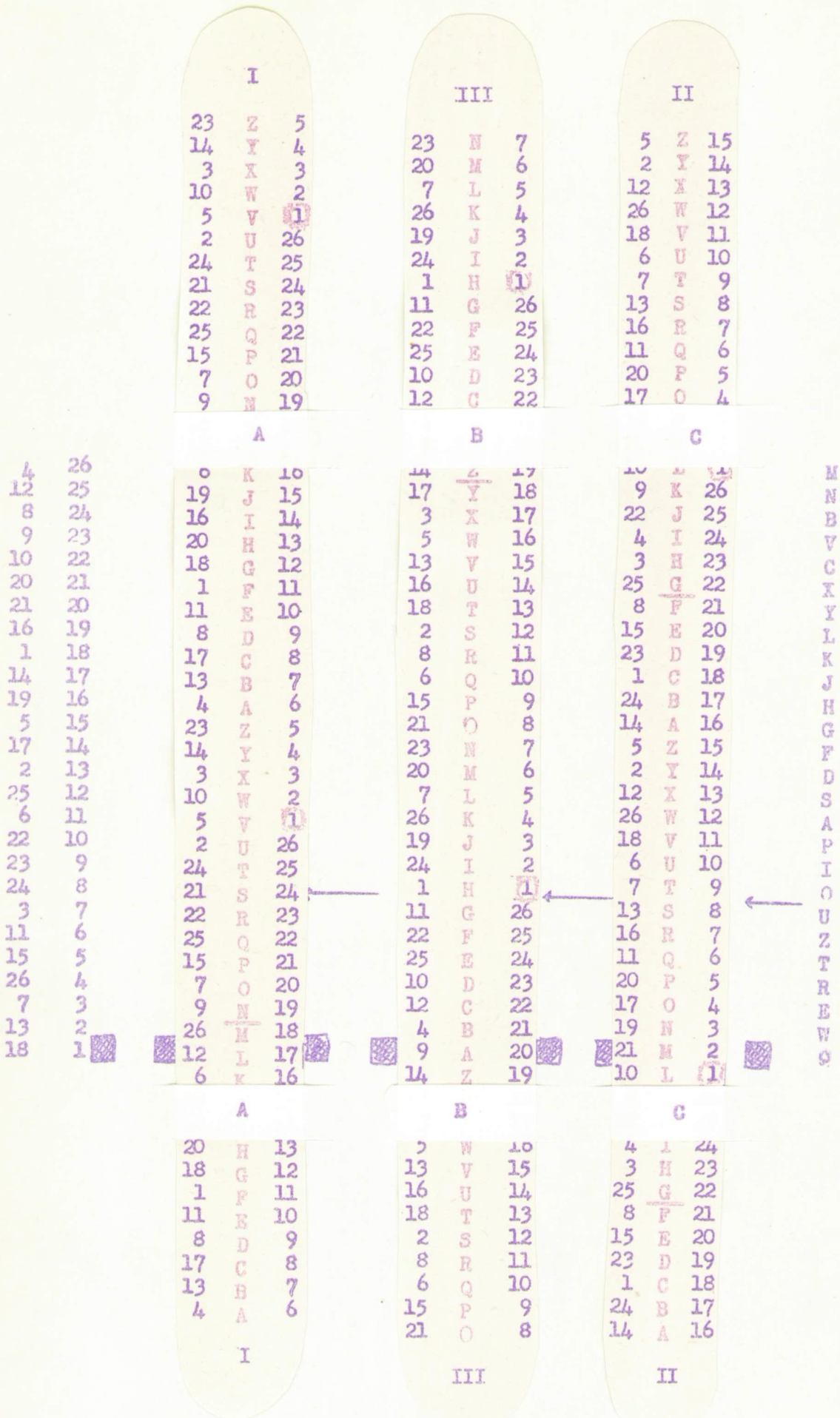


App. III A1

TOP SECRET

Doc ID: 6592463

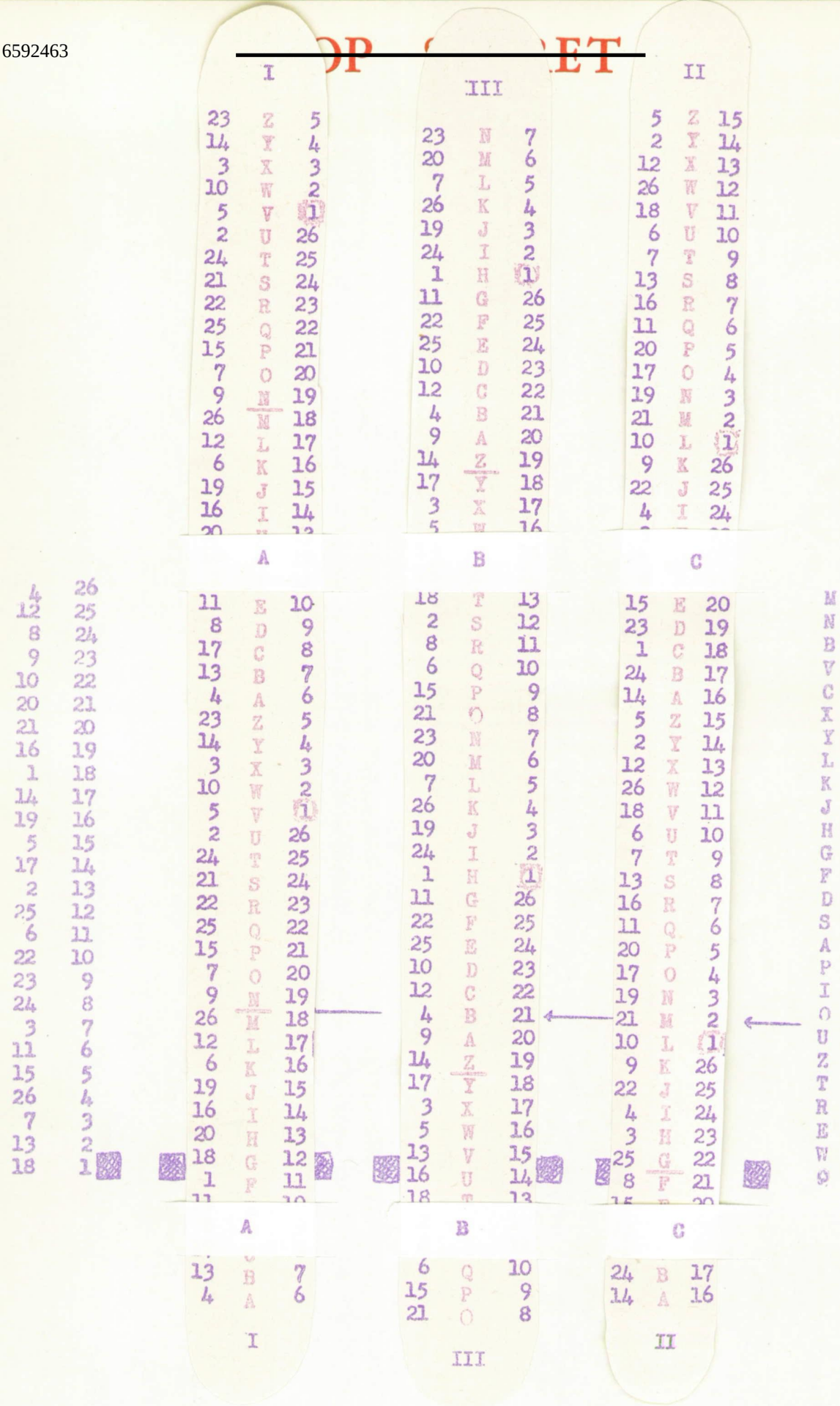
TOP SECRET



TOP SECRET

Doc ID: 6592463

TOP SECRET



(American analogue)

TOP SECRET

Doc ID: 6592463

TOP SECRET

I n																										
III c																										
II f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e
	21	22	23	24	25	26	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
m	s	l	l	c	p	w	g	i	v	w	p	z	f	o	b	b	c	h	d	w	c	x	p	q	l	t
n	d	r	t	i	c	j	a	v	p	y	z	h	w	d	l	p	b	f	k	r	x	h	c	b	a	g
b	x	j	c	x	g	l	i	s	j	v	p	u	c	g	m	m	n	r	c	l	d	r	o	n	r	j
v	f	h	w	o	t	g	e	n	m	b	e	p	t	i	a	f	k	g	s	f	a	u	a	s	f	u
c	t	a	b	m	n	r	j	z	h	z	x	a	b	y	g	a	m	j	b	k	m	e	n	x	e	r
x	b	p	z	b	w	i	s	h	l	p	c	r	e	f	h	k	y	y	o	u	n	m	u	c	h	p
y	g	q	r	r	a	t	w	j	z	n	u	g	g	c	i	l	x	x	l	p	l	f	f	d	k	h
l	w	m	m	u	j	b	r	o	x	r	o	j	k	q	n	y	h	q	y	b	y	d	s	f	m	k
k	r	o	j	j	f	d	f	q	u	d	f	q	l	u	o	x	v	i	n	c	q	z	t	i	y	l
j	o	b	k	k	l	n	c	y	b	a	s	l	u	z	r	u	a	c	i	z	h	g	q	a	q	b
h	a	v	e	g	d	s	o	x	c	s	b	n	d	e	x	i	l	m	p	g	j	n	e	z	x	y
g	y	e	u	h	b	v	m	w	e	t	i	y	y	b	c	q	u	v	q	h	t	j	i	e	p	n
f	v	s	p	e	k	e	k	e	s	i	k	o	m	x	t	v	p	n	u	v	z	y	y	l	v	z
d	n	t	s	w	h	k	q	t	r	k	r	t	h	n	u	z	s	t	m	a	b	l	r	y	u	s
s	m	f	d	a	q	h	x	b	f	h	j	w	i	t	w	w	d	o	v	o	p	t	l	v	z	d
a	h	c	o	s	y	q	n	u	w	j	q	c	q	r	v	c	j	e	r	d	v	o	v	j	n	q
p	e	x	f	q	m	o	z	r	n	x	m	v	o	w	e	n	f	u	h	y	s	w	m	u	g	x
i	u	w	q	n	r	x	b	m	o	f	g	e	s	v	y	h	z	k	j	e	u	q	g	k	t	w
o	j	k	a	v	e	p	h	l	i	u	l	f	p	m	p	t	t	s	x	s	e	a	b	w	w	e
u	i	z	g	l	z	z	t	a	k	o	y	b	j	k	d	j	g	p	f	x	i	v	x	p	d	v
z	q	u	x	t	u	u	p	c	y	c	n	m	r	j	q	d	i	w	w	j	f	k	w	h	s	f
t	c	d	n	z	v	y	u	d	q	g	w	d	v	s	f	o	o	d	e	q	g	s	k	r	i	m
r	k	n	y	y	i	c	l	p	d	l	d	x	z	a	j	e	q	b	a	n	w	b	d	t	b	c
e	p	g	h	f	o	f	v	f	g	q	v	i	x	h	p	r	w	a	t	i	o	c	h	g	c	o
w	l	i	v	d	x	m	y	g	a	m	t	s	n	p	s	s	e	z	z	m	r	p	z	o	o	i
q	z	y	i	p	s	a	d	k	t	e	a	k	a	l	z	g	r	l	g	t	k	i	j	m	j	a

TOP SECRET

Doc ID: 6592463

				21	22	23	24	25	26	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
a	5	m	20	6	13	13	16	4	22	9	3	17	22	4	26	8	2	18	18	16	10	7	22	16	15	4	21	13	25
b	18	n	19	7	24	25	3	16	11	5	17	4	14	26	10	22	7	13	4	18	8	12	24	15	10	16	18	5	9
c	16	b	18	15	11	16	15	9	13	3	6	11	17	10	1	16	9	20	20	19	24	16	13	7	24	2	19	24	11
d	7	v	17	8	10	22	2	25	9	23	19	20	18	23	4	25	3	5	8	12	9	6	8	5	1	5	6	8	1
e	23	c	16	25	5	18	20	19	24	11	26	10	26	15	5	18	14	9	5	20	11	18	12	20	23	19	15	23	24
f	8	x	15	18	4	26	18	22	3	6	10	13	4	16	24	23	8	10	12	14	14	2	1	19	20	1	16	10	4
g	9	y	14	9	21	24	24	5	25	22	11	26	19	1	9	9	16	3	13	15	15	13	4	13	8	8	7	12	10
h	10	l	13	22	20	20	1	11	18	24	2	15	24	2	11	12	21	19	14	10	21	14	18	14	7	6	8	20	12
i	3	k	12	24	2	11	11	8	7	8	21	1	7	8	21	13	1	2	15	17	3	19	16	21	26	25	3	14	13
j	11	j	11	2	18	12	12	13	19	16	14	18	5	6	13	1	26	24	1	5	16	3	26	10	9	21	5	21	18
k	12	h	10	5	17	23	9	7	6	2	15	16	6	18	19	7	23	15	3	13	20	4	9	11	19	23	26	15	14
l	13	g	9	14	23	1	10	18	17	20	22	23	25	3	14	14	18	16	21	1	17	21	10	25	11	3	23	4	19
m	20	f	8	17	6	4	23	12	23	12	23	6	3	12	2	20	15	25	17	4	19	1	17	26	14	14	13	17	26
n	19	d	7	19	25	6	22	10	12	21	25	24	12	24	25	10	19	1	26	6	25	20	5	18	13	24	14	1	6
o	2	s	6	20	8	7	5	21	10	15	18	8	10	11	22	3	25	22	22	7	2	17	2	4	25	13	17	26	7
p	4	a	5	10	16	2	6	14	21	19	1	22	11	21	16	21	24	17	16	11	23	24	7	17	2	17	11	19	21
q	21	p	4	23	15	8	21	20	2	26	24	19	15	20	17	2	22	23	19	8	1	10	14	6	22	20	1	9	15
r	24	i	3	1	22	21	19	24	15	18	20	2	8	9	23	6	17	14	10	26	12	11	23	1	21	9	12	25	22
s	6	o	2	11	12	5	17	23	4	10	13	3	1	13	8	4	20	12	25	25	6	15	6	23	5	18	22	22	23
t	25	u	1	3	26	9	13	26	26	25	5	12	2	14	18	11	12	7	11	9	4	8	15	3	17	15	4	7	17
u	1	z	26	21	1	15	25	1	1	4	16	14	16	19	20	24	11	21	7	3	22	22	11	8	12	22	10	6	8
v	17	t	25	16	7	19	26	17	14	1	7	21	9	22	7	17	6	8	2	2	7	23	21	9	6	12	24	3	20
w	22	r	24	12	13	14	14	3	16	13	4	7	13	7	15	26	5	11	23	21	18	5	19	22	18	7	25	18	16
x	15	e	23	4	3	10	8	2	8	17	8	9	21	17	3	15	10	4	24	22	5	25	3	2	16	10	9	16	2
y	14	w	22	13	3	17	7	15	20	14	9	5	20	25	6	19	4	6	6	23	26	26	20	24	4	26	2	2	3
z	26	q	21	26	14	3	4	6	5	7	12	25	23	5	12	5	13	26	9	24	13	9	25	12	3	11	20	11	5

TOP SECRET

TOP SECRET

3

Doc ID: 6592463

	21	22	23	24	25	26	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
+	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
20	6	14	15	19	8	1	15	10	25	5	14	11	20	15	6	7	6	1	25	15	10	10	26	18	11	24
19	7	25	1	6	20	16	11	24	12	23	10	21	8	20	1	19	8	25	4	17	9	5	12	15	3	8
18	15	12	18	18	13	18	9	13	19	26	20	12	2	22	8	9	9	15	8	6	1	19	24	16	22	10
17	8	11	24	5	3	14	3	26	2	1	7	15	11	16	19	23	2	26	24	1	25	22	1	3	6	26
16	25	6	20	23	23	3	17	7	18	9	25	16	4	1	23	20	10	2	10	5	14	18	15	12	21	23
15	18	5	2	21	26	8	12	17	21	13	26	9	9	21	24	1	4	5	20	20	13	15	23	13	8	3
14	9	22	26	1	9	4	2	18	8	2	11	20	21	3	17	2	5	6	5	23	7	3	4	4	10	9
13	22	21	22	4	15	23	4	9	23	7	12	22	24	8	7	3	26	12	6	11	18	2	2	5	18	11
12	24	3	13	14	12	12	14	2	9	16	17	6	25	14	16	4	7	20	11	3	15	21	21	26	12	12
11	2	19	14	15	17	24	22	21	26	14	16	24	13	13	12	16	21	7	21	13	4	4	17	2	19	17
10	5	18	25	12	11	11	8	22	24	15	2	4	19	10	3	18	3	11	22	2	5	14	19	23	13	13
9	14	24	3	13	22	22	26	3	5	8	13	25	26	5	4	10	17	8	13	3	19	6	25	20	2	18
8	17	7	6	26	16	2	18	4	14	12	22	13	6	2	13	6	20	10	19	10	20	9	10	10	15	25
7	19	26	8	25	14	17	1	6	6	21	8	10	22	6	15	15	22	16	12	24	12	8	20	11	25	5
6	20	9	9	8	25	15	21	25	16	19	21	7	15	12	10	11	23	19	9	21	24	20	9	14	24	6
5	10	17	4	9	18	26	25	8	4	20	5	1	7	11	5	5	1	14	16	26	11	23	13	8	17	20
4	23	16	10	24	24	7	6	5	1	24	4	2	14	9	11	8	24	18	2	7	26	17	16	24	7	14
3	1	23	23	22	2	20	24	1	10	17	19	8	18	4	2	25	16	3	3	16	21	16	5	9	23	21
2	11	13	7	20	1	9	16	20	11	10	23	19	16	7	26	14	15	23	7	25	17	26	14	19	20	22
1	3	1	11	16	4	5	5	12	20	11	24	3	23	25	21	26	25	21	26	8	23	12	11	1	5	16
26	21	2	17	2	5	6	10	23	22	25	3	5	10	24	9	22	19	13	14	4	2	7	18	7	4	7
25	16	8	21	3	21	19	7	14	3	18	6	18	3	19	22	17	18	24	15	14	3	1	8	21	1	19
24	12	20	16	17	7	21	19	11	15	22	17	26	12	18	25	12	11	9	23	12	16	13	3	22	16	15
23	4	10	12	11	6	13	22	15	17	4	1	14	1	23	18	13	12	22	17	22	22	11	6	6	14	1
22	13	4	19	10	19	25	20	16	13	3	9	17	5	17	20	21	13	17	18	13	18	25	22	25	26	2
21	26	15	5	7	10	10	13	19	7	6	15	23	17	26	14	24	14	4	1	18	6	24	7	17	9	4

TOP SECRET

TOP SECRET

4

Doc ID: 6592463

TOP SECRET

20	6	25	18	5	23	8	2	9	9	14	2	25	6	6	10	5	24	3	7	8	2	1	3	6	26	4
19	7	12	24	23	26	4	4	2	26	15	13	13	22	12	5	8	16	23	26	4	3	13	6	25	9	24
18	15	11	20	21	9	23	14	21	24	8	22	10	15	11	11	25	15	21	14	14	16	11	22	17	11	8
17	8	6	2	1	15	12	22	22	5	12	8	7	7	9	2	14	25	13	15	12	22	25	7	18	3	10
16	25	5	26	4	12	24	8	3	14	21	21	1	14	4	26	26	19	24	23	22	18	24	26	15	22	26
15	18	22	22	14	17	11	26	4	6	19	5	2	18	7	21	22	18	9	17	13	6	10	12	16	6	23
14	9	21	13	15	11	22	18	6	16	20	4	8	16	25	9	17	11	22	18	18	10	5	24	3	21	3
13	22	3	14	12	22	2	1	25	4	24	13	13	23	24	22	12	12	17	1	15	9	13	1	12	8	9
12	24	13	25	13	16	17	21	8	1	17	23	3	10	13	25	13	13	4	25	17	1	22	15	13	10	11
11	2	18	3	26	14	15	25	5	10	10	24	5	3	18	18	21	14	1	4	6	25	18	23	4	18	12
10	5	24	6	25	25	26	6	1	11	11	3	18	12	23	20	24	6	25	8	1	14	15	4	5	12	17
9	14	7	8	8	18	7	24	20	20	25	6	26	1	17	14	7	8	15	24	5	13	3	2	26	13	13
8	17	26	9	9	24	20	16	12	22	18	17	14	5	26	6	19	9	26	10	20	7	2	21	2	13	18
7	19	(9)	4	24	[2]	(9)	5	(23)	3	22	(1)	17	[17]	15	(1)	(9)	2	[2]	20	(23)	8	21	17	23	2	25
6	20	17	(10)	22	1	[5]	(10)	14	(15)	4	9	(23)	20	20	8	(23)	(10)	[5]	5	11	(13)	4	19	20	15	5
5	10	16	23	20	4	6	7	11	17	3	15	11	8	22	19	20	4	6	6	9	4	14	25	10	25	6
4	23	23	7	16	5	19	19	15	13	6	14	21	2	16	23	1	5	12	11	19	5	6	10	11	24	20
3	1	13	11	2	21	21	23	16	7	5	10	12	11	1	24	2	26	20	21	2	19	9	20	14	17	14
2	11	1	17	3	7	13	20	13	25	23	20	15	4	21	17	3	7	7	22	3	20	8	9	8	7	21
1	3	2	21	17	6	25	13	10	12	26	7	16	9	3	7	4	21	11	13	10	12	20	13	24	23	22
26	21	8	16	11	13	10	15	24	19	1	25	9	21	8	16	16	3	8	19	24	24	23	16	9	20	16
25	16	20	12	10	10	1	11	13	2	9	26	20	24	14	12	18	17	10	12	21	11	17	5	19	5	7
24	12	10	13	7	8	16	9	26	18	13	11	22	25	13	3	10	20	16	9	26	26	16	14	1	4	13
23	4	4	5	19	20	18	3	7	21	2	12	6	13	10	4	6	22	19	16	7	21	26	11	7	1	15
22	13	15	15	6	13	14	17	17	8	7	18	24	19	5	13	15	23	14	2	16	17	12	18	21	16	1
21	26	14	1	18	3	3	12	18	23	16	16	4	26	2	15	11	1	18	3	25	23	7	8	22	14	2

23

TOP SECRET

5

Doc ID: 6592463

TOP SECRET

17	26
4	25
3	24
19	23
6	22
7	21
12	20
23	19
8	18
26	17
11	16
9	15
5	14
2	13
20	12
16	11
1	10
15	9
18	8
21	7
22	6
14	5
25	4
24	3
13	2
10	1

Reversing mirror of the wheel complex consisting of the reversing wheel
Wheel I
Wheel III
with the window setting n c f

9
21
21
4
16
14
8
22
10
17
5
6
9
11
18
21
9
20
16
12
10
17
5
5
15
17

Same reversing mirror, but expressed in the difference values between the contacts.

18
22
22
14
17
11
26
4
6
13
5
2
18
7
21
22
18
9
17
13
6

Row 15
from Sheet 5

10
16
23
20
4
6
7
11
17
3
15
11
8
22
19
20
4
6
6
9
4

Row 5
from Sheet 5

TOP SECRET

Doc ID: 6592463

TOP SECRET

15	18	22	22	14	17	11	26	4	6	19	5	2	18	7	21	22	18	9	17	13	6	10	12	16	6	23
23	4	4	5	19	20	18	3	7	21	2	12	6	13	10	4	6	22	19	16	7	21	26	11	7	1	15
1	3	2	21	17	6	25	13	10	12	26	7	16	9	3	7	4	21	11	13	10	12	20	13	24	23	22
24	12	10	19	7	8	16	9	26	18	13	11	22	25	13	3	10	20	16	9	26	26	16	14	1	4	19
14	9	21	13	15	11	22	18	6	16	20	4	8	16	25	9	17	11	22	18	18	10	5	24	3	21	3
5	10	16	23	20	4	6	7	11	17	3	15	11	8	22	19	20	4	6	6	9	4	14	25	10	25	6
2	11	1	17	3	7	13	20	19	25	23	20	15	4	21	17	3	7	7	22	3	20	8	9	8	7	21
12	24	19	25	13	16	17	21	8	1	17	23	3	10	19	25	13	13	4	25	14	1	22	15	13	10	11
26	21	8	16	11	19	10	15	24	19	1	25	9	21	8	16	16	3	8	19	24	24	23	16	9	20	16
18	15	11	20	21	9	23	14	21	24	8	22	10	15	11	11	25	15	21	14	14	16	1	22	17	1	8
6	20	17	10	22	1	5	10	14	15	4	9	23	20	20	8	23	10	5	5	11	15	4	19	20	15	5
7	19	9	4	24	2	9	5	23	3	22	1	17	17	15	1	9	2	2	20	23	8	21	17	23	2	25
13	22	3	14	12	22	2	1	25	4	24	19	19	23	24	22	12	12	17	1	15	9	19	1	12	8	9
16	25	5	26	4	12	24	8	3	14	21	21	1	14	4	26	26	19	24	23	22	18	24	27	15	22	28
11	2	18	3	26	14	15	25	5	10	10	24	5	3	18	18	21	14	1	4	6	25	18	23	4	18	12
20	6	25	18	5	23	8	2	9	9	14	2	25	6	6	10	5	24	3	7	8	2	1	3	6	26	4
17	8	6	2	1	15	12	22	22	5	12	8	7	7	9	2	14	25	13	15	12	22	25	7	18	3	10
19	7	12	24	23	26	4	4	2	26	15	13	13	22	12	5	8	16	23	26	4	3	13	6	25	9	24
21	26	14	1	18	3	3	12	18	23	16	16	4	26	2	15	11	1	18	3	25	23	7	8	22	14	2
10	5	24	6	25	25	26	6	1	11	11	3	18	12	23	20	24	6	25	8	1	14	15	4	5	12	17
9	14	7	8	8	18	7	24	20	20	25	6	26	1	17	14	7	8	15	24	5	13	3	2	26	19	13
22	13	15	15	6	13	14	17	17	8	7	18	24	19	5	13	15	23	14	2	16	17	12	18	21	16	1
4	23	23	7	16	5	19	19	15	13	6	14	21	2	16	23	1	5	12	11	19	5	6	10	11	24	20
3	1	13	11	2	21	21	23	16	7	5	10	12	11	1	24	2	26	20	21	2	19	9	20	14	17	14
25	16	20	12	10	10	1	11	13	2	9	26	20	24	14	12	18	17	10	12	21	11	17	5	19	5	7
8	17	26	9	9	24	20	16	12	22	18	17	14	5	26	6	19	9	26	10	20	7	2	21	2	13	18

25

TOP SECRET

Doc ID: 6592463

TOP SECRET

Appendix III A 1 e, Sheet 8
Fuligme Type K

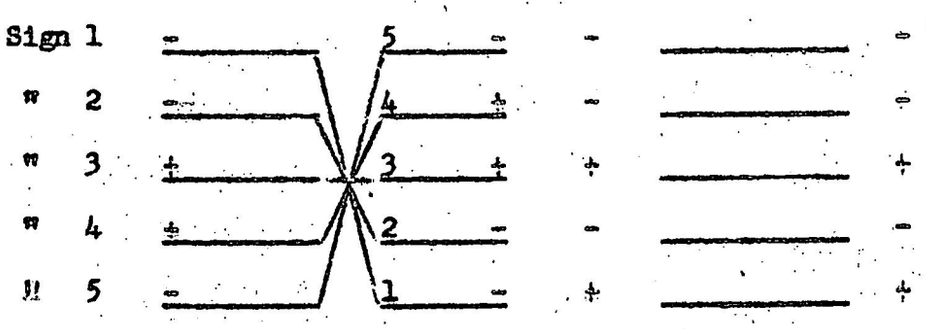
TOP SECRET

2. The Siemens Cipher Teleprinters

Die Siemens-Geheim-Fernschreibmaschinen

The construction and functioning of the Siemens Cipher Teleprinters is likewise assumed to be known. Encipherment is based on the following principle:

32 plain elements in all are converted into five + and - signs of the baudot alphabet. These signs run first over five wheels, which according to their cam pattern cause a transposition of the signs, and then over five other wheels which according to the cam pattern either convert the already transposed signs into their opposite or leave them without further change. Hence we have a combination of transpositions and substitutions. Expressed in the form of a diagram we get:



The plain signs or impulses 1 2 3 4 5, which in the above diagram read - - + + -, are shifted at the point marked U corresponding to the existing cam pattern to - + + - - and at the point marked E are either left unchanged if they coincide with the sign of the second set of five wheels, or are replaced by the opposite sign, if unlike signs come together.

The possibilities of solution depend on the following consideration:

The baudot alphabet from the point of view of cryptography is by no means calculated to equalize the frequency of the + or - impulses in the first to fifth positions, having regard for the frequencies of the plain language. On the contrary, for practical reasons it is so constructed that the most frequent plain letters show the least number of plus impulses.

Consequently by taking into consideration the frequencies of the plain language it is possible to calculate what percent of plus impulses and minus impulses appear in the first to fifth positions.

It is also necessary to ascertain which switches at position U on the diagram correspond to the 32 possible combinations of cam crest and cam trough on the five wheels of the cipher teleprinter SFM 52 Type ab.

From these two basic computations it is then possible to compute how the minus impulses of level 1 are conducted through the various switch arrangements to levels 1 to 5. If this computation is then carried out for levels 2 to 5, then we know the percentage of plus and minus impulses to be expected for each individual level at position E. If it turns out that at position E some 60 percent minus impulses and 40 percent plus impulses enter on the average, it can be deduced from that that the first impulse of the cipher text, if superimposed in ten columns corresponding to the "length" of the ten wheels, must necessarily give a reflection of the wheel in question in one of these ten cases (namely when the column width of the text and the pattern (Umfang) of the wheel active at that point in the diagram agree) whereby the crest or trough and the predominance of minus or plus impulses must correspond.

Since the cams on the wheels of the SFM 52 Type a/b are not settable i.e., are invariable, it is necessary when testing the security of the machine to start with the assumption that the wheels are known to the unauthorized cryptanalyst.

Consequently a comparison of the above texts written out in various column widths with the cam patterns of the wheels can show which five wheels are active at position E and what their initial setting is. Using these wheels the cipher text can be converted into an intermediate text which differs from the plain text only by the transposition (Umstellung).

A comparison of the intermediate text, written down according to the patterns of the five remaining wheels, with the other five wheels leads to the solution of the plain text if we consider the plain elements arising.

Instead of computing the probabilities for the distribution of plus and minus impulses, the necessary preliminary work may be done by studying a plain text of sufficient length, say 10,000 letters, to determine the distribution of the impulses at different points in the diagram.

The effect of the regularities inherent in the machine on the one hand, and of the regularities resulting from the plain text frequencies in conjunction with the baudot alphabet on the other hand, is so strong that a cipher text produced by the SFM 52 Type ab can be worked on with good prospect of success if it is 500 elements in length.

Much more simple is the solution of the SFM 52 Type c. This new type, supposedly developed as an improvement on Type a/b differs essentially only in the wirings effective at point U of the diagram as these are activated by the cam pattern of the wheels involved.

In the supposed improvement one factor was overlooked, namely how these new wirings would affect the cipher text. Even a simple study to see which cipher values can occur in enciphering a given letter would have shown that from one plain letter we cannot get all 32 possible cipher values but that only 16 different letters are possible as encipherment for any plain letter. Further experiments of this sort would have shown that, due to pecularities in the wiring found in Type c, the 32 letters fall into two separate cycles, and a plain value from one cycle can only be enciphered by values from the same cycle.

Since about 15 letters of continuous enciphered text with known plain text will suffice for computing the setting of the machine, there is a much simpler method of solution for the Type c.

This consists in converting the supposed plain text passage of this length (crib) and the cipher text itself into the digits 1 and 2, according to the cycle to which the letter involved belongs. A comparison of the assumed plain text thus converted into digits with the cipher text shows whether and in what position this assumption may fit. Further computation then shows whether the assumption is correct or not.

The Siemens Cipher Teleprinters were capable of solution then because

1. Both Types a/b and Type c use wheels with fixed cam patterns which cannot be varied;
2. The wheel stepping is absolutely uniform in both types so that the cipher text can be written out on widths corresponding to the lengths of the wheels;
3. The baudot alphabet with its distribution of plus and minus impulses is used rather than some special alphabet which would correspond to cryptologic demands;
4. The internal wiring of Type c was poorly chosen.

Due to the combination of all these defects it was not possible for the essentially sound principle of combining substitution and transposition within the polyalphabetic substitutions to realize its advantages.

The two types d and e represent an emergency solution which had to be adopted when it appeared that the existing types could not meet security demands. Since one could not think of a new construction under the circumstances, the only thing left was a reconstruction of the existing devices and possible improvements were greatly limited by technical restrictions.

The improvements consisted ultimately only in the introduction of a supplemental device which changed the hitherto regular wheel stepping through the interaction of the wheels. By the installation of this supplemental device Type a/b became Type d and Type c became Type e getting a new wiring at the same time.

No final investigation of the degree of security thus obtained was ever made.

3. The Army Supplemental Device.

The last of the cipher machines used by the German Armed Forces was the so-called Army Supplemental Device T 42, details of which never became known to the writer.* The cipher part of the device was combined with a punched tape printer to which the cipher text was transferred. For transmitting the punched tape plain teleprinters could be used.

The possibility of solution again lay in the fact that the supplemental device, like the Enigma and the Siemens Cipher Teleprinters, used only fixed parts which could not be set at will.

* The translator also has no further information.

SECTION B

NON-GERMAN CIPHER MACHINES

While all German cipher machines suffered from the serious defect that the individual parts which accomplished the encipherment were rigid, hence were not settable, and that the stepping of the machines was regular, most of the non-German manufacturers succeeded in overcoming these defects in the course of time by further development.

1. The Japanese Cipher Machine.

The construction and functioning of the Japanese cipher machine never became known to the German cryptologists, nor was it ever possible to learn from the cipher text with any high degree of probability how the machine must have been constructed.

From a standpoint of characteristics this machine occupies a special position since it is the only one known which is based upon the principle of the short slide. Actually several 2-part slides are involved which are arranged one after the other, one part originally had only the twenty consonants and the other part only the six vowels. The machine passed through several stages of development, some so related that a new stage of development often could only be recognized after the next had been reached. The fact that several 2-part slides must have been arranged one after the other was not recognized until late, because - for practical purposes - a single 2-part slide would have the same effect. The letters on the slides could be inscribed in any desired sequence.

In the first development stage the plain sequences of both partial slides are displaced one letter with respect to the cipher sequence after enciphering an element. Consequently, what we have is a columnar polyalphabetic substitution (Spaltencäsar) corresponding to the Tritheim table. Solution is possible on the basis of isomorphic passages in the cipher text.

It is greatly facilitated by the appearance of stereotype message beginnings. The Japanese characters are converted into a kana-alphabet which is made up of two-place syllables containing one consonant and one vowel.

At the next stage of development a slight change appears in that consonants and vowels occur on the longer as well as on the shorter part of the slide. The plain sequences of the slides may show skips of two or three cells instead of the normal step of one cell as measured on the cipher sequence. Within a regular route (Turnus) of 42 (?) letters only two different types of skip appear, in each case with two to three simple and one to two double steps at definite intervals. Consequently this is a very feebly irregular skip system. Consequently the possibilities of solving the cipher text were hardly affected. The different daily keys can be derived from one another within a decade (10 day period: from the 1st to the 10th, 11th to 20th, 21st to 30th of the month) through a 2-part decade key, so that solution of one message within a decade is sufficient to permit reading all traffic of this decade. During a period of two years the decade keys for a half year could be derived from a common half year key and the two half year keys from an annual key. Later on, a common annual key could not be recognized.

About 1942 a new difficulty appeared, inasmuch as all typical telegram beginnings and common words were replaced by 3-place code groups, some of which were taken from the international Q-groups. Isomorphic parallel passages become less frequent and solution is consequently somewhat more laborious.

From about 1943 on, the cipher text could no longer be solved. Outwardly the messages did not differ in any way from the earlier traffic so that it was natural to assume that the same machine was involved, but in a much improved version although no proof of this could be obtained.

Doc ID: 6592463

Assuming that the machine was based on the same principle, a study of the cipher text and particularly of the isomorphic passages allows the deduction that the hitherto feebly irregular skip system has been replaced by a very irregular skip system with short and long skip intervals (in case the plain text has not been enciphered according to some other system before being enciphered with the machine).

2. The Hagelin Cipher Machines.

The Swedish Hagelin machines which are available in the open market have had a wider distribution, and a special model is used on a large scale by the American army.

An older model of the Swedish Hagelin Company and a quite different although less secure model put out by the French Hagelin Company cannot be treated here because these models are not known to the author. The fairly recent model of 1939 reveals as essential cipher parts 6 variable pin wheels and the so-called basket (cage) on the bars of which are found a considerable number of lugs which can be set corresponding to the different wheels. The number of lugs runs up to 27. With each revolution of the wheels and the associated revolution of the basket which takes place after the encipherment of each letter, those lugs became effective which encounter a pin projection on the corresponding wheel. If the pin projections on the wheels are represented by a plus and the absence of pin projections by a minus and the lugs are set, let us say, with respect

to wheels		I	II	III	IV	V	VI	
in each case	a)	8	7	6	3	2	1	= 27
or	b)	22	1	1	1	1	1	= 27
or	c)	4	4	4	4	4	7	= 27

Then with the following pin patterns on the 6 wheels the following number of lugs will be effective:

Pin setting	Number of lugs a)	b)	c)	Pin setting	Number of lugs a)	b)	c)
- - - - - -	0	0	0	+ + + + + +	27	27	27
- - - - - +	1	1	7	+ + + + + -	26	26	20
- - - - + -	2	1	4	+ + + + - +	25	26	23
- - - + - -	3	1	4	+ + + - + +	24	26	23
- - - - + +	3	2	11	+ + + + - -	24	25	16
- - - + - +	4	2	11	+ + + - + -	23	25	16
- - - + + -	5	2	8	+ + + - - +	22	25	19
- - + - - -	6	1	4	+ + - + + +	21	26	23
- - - + + +	6	3	15	+ + + - - -	21	24	12
- + - - - -	7	1	4	+ - + + + +	20	26	23
- - + - - +	7	2	11	+ + - + + -	20	25	16
+ - - - - -	8	22	4	- + + + + +	19	5	23
- + - - - +	8	2	11	+ - + + + -	19	25	16
- - + - + -	8	2	8	+ + - + - +	19	25	19
+ - - - - +	9	23	11	- + + + + -	18	4	16
- + - - + -	9	2	8	+ - + + - +	18	25	19
- - + + - -	9	2	8	+ + - - + +	18	25	19
- - + - + +	9	3	15	+ + - + - -	18	24	12
+ - - - + -	10	23	8	- + + + - +	17	4	19
- + - + - -	10	2	8	+ - + - + +	17	25	19
- + - - + +	10	3	15	+ - + + - -	17	24	12
- - + + - +	10	3	15	+ + - - + -	17	24	12
+ - - + - -	11	23	8	- + + - + +	16	4	19
+ - - - + +	11	24	15	- + + + - -	16	3	12
- + - + - +	11	3	15	+ - + - + -	16	24	12
- - + + + -	11	3	12	+ + - - - +	16	24	15
+ - - + - +	12	24	15	- + + - + -	15	3	12
- + - + + -	12	3	12	+ - + - - +	15	24	15
- - + + + +	12	4	19	+ + - - - -	15	23	8
- + + - - -	13	2	8	+ - - + + +	14	25	19
+ - - + + -	13	24	12	- + + - - +	14	3	15
- + - + + +	13	4	19	+ - + - - -	14	23	8

Since the alphabet has 25 (26?) letters and the effective lugs indicate how many letters one is to count ahead in the alphabet in order to reach the cipher letter, any letter - according to the lug position - can become a cipher letter, as is the case with lug setting a. Examples b and c show that there are also very unfavorable lug settings.

The wheels of the Hagelin machine have a regular stepping, i.e., they move after the encipherment of an element. The total period of the one step machine is fairly large since the wheel lengths have no common factors and consequently the period of the machine is the product of the lengths of the six wheels.

Since what we have is a systematic polyalphabetic substitution (Spaltencæsar) with a known alphabet sequence, there is a possibility of solution corresponding to what we have learned in connection with polyalphabetic substitution (Spaltencæsar) as soon as at least two messages in the same key are found.

There is a second possibility of solution if we have continuous enciphered texts of a certain minimum length, this minimum depending on the more or less favorable distribution of the lugs on the bars and ranging between 3,000 and 8,000 letters.

If the entire cipher text is scored in six rectangles with column widths corresponding to the length - i.e., the possible positions - of the six wheels, with 25 rows corresponding to the cipher elements a to z, then in the 25 rows of each rectangle the resulting high or low scores in the cells will reflect the pin pattern of the wheels concerned in such fashion that in the one row the heavily scored cells will reflect the pins in effective position on the wheel while in another row this will be shown by the lightly scored cells. Of course this reflection of the pin pattern is not equally well impressed on each row, nevertheless by evaluating all the rows of a rectangle simultaneously one can recognize with a high degree of probability the pin pattern of the wheel and also its initial position. All that remains unknown is whether the total result from the 25 rows of the rectangle is the direct or the inverted picture of the pin pattern. Hence there are $26 = 64$ possibilities of setting up the pins on the wheel.

The study of the 64 possible pin patterns in connection with the cipher text, taking into account the plain text frequency, affords a possibility of determining the number of lugs associated with the individual wheels, whereupon the cipher text can be deciphered with the machine.

Of course, two methods of solution are involved which are tied to assumptions which could easily be avoided by the cipher clerk so that these are really theoretical possibilities of solution which occur only where there has been carelessness in enciphering.

So it happens even with this relatively good cipher machine, whose security is to be rated high, that the two remaining methods of solution both start with regularities inherent in the machine, namely the

columnar substitution alphabet (Spaltencäsar), which has for all columns the same sequence of letters simply with a different displacement, and the regular stepping of the six wheels. If the individual alphabets were to have a structure which differed from day to day at least and if the stepping of the wheels were irregular and random, then these two methods of solution would be ruled out.

3. The Russian Multi-channel Radio Cipher Teleprinter

During the last world war multi-channel radio cipher teleprinters were developed in Russia. In one case a plain text printer and a cipher text printer are coupled synchronously, while in the second case a plain text printer and eight cipher printers are synchronized so that all machines were sending in the radio alphabet at the same tempo (when the machine is not in use then - - - - - etc., was sent irrespective of whether the individual machines were used for sending or not). The various plus and minus impulses were so scrambled with one another before transmission in both the 2-channel and the 9-channel machine that, when received, a technical unscrambling was necessary before a cipher text capable of expression in letters resulted for the several cipher channels. This cipher text could then be worked on by the cryptanalysts.

For receiving the two-channel text a receiver was constructed which automatically undertook the unscrambling so that the machine provided a plain text and a cipher text.

Both texts indicated the pauses in transmission by - - - - - etc. The cipher tape has the peculiarity that in passing from the preliminary call-up to the transmission pause, the Russian letter П, represented in the radio alphabet by + + + + -, occurs seven times. On the other hand when passing from the transmission pause after the preliminary call-up, during which pause the prearranged cipher key was set up on the machine, to the cipher text, this seven-fold repetition of the same letter no longer appears nor did it when passing from the cipher traffic to the transmission pause.

Doc ID: 6592463

Now since it was natural to assume that in this transition to and from cipher texts the same letter ⌐ = + + + + + likewise appeared seven times in each case but was no longer recognizable due to the encipherment, the first and last seven cipher values of all cipher texts interrupted by transmission pauses were subjected to special study. Since the machine, once the daily key had been set up, was used very frequently during the course of the day for sending cipher text with numerous pauses in transmission without any new daily key being set up, rather numerous fragments of a length of seven letters were available at known intervals of greater or lesser lengths.

The assumption, which at first was merely a vague one, became a certainty when once, after the sending and receiving machines had gotten out of step, an already used key was set up on the machine for the second time and now not merely the first seven letters corresponded when passing to the first cipher text but in addition the change from cipher text to transmission pause of one cipher text and the change from the transmission pause to the cipher text of the second cipher text coincided in the first four letters of the first transmission with the last four letters of the second transmission and a count of the intervals of the two transmissions, counting each time from the beginning of the cipher text, showed a difference of three.

From this it could be concluded that the first seven and the last seven letters of each secret text came from enciphering the letter ⌐ = + + + + + seven times and hence these fragments of cipher text represented pure key text. The following study of these fragments of pure key text led to a recognition of the fact that the first impulses show the same repeated picture in the chain of plus and minus impulses at an interval of 37, the second impulses at an interval of 39, the third impulses at an interval of 41, the fourth and fifth at an interval of 43 and 45 respectively (the intervals may have been 35, 37, 39, 41, 43). This showed the length of the five cipher wheels and their cam pattern according to the day's setting. Each cam crest caused the

inversion of the plain impulse into its opposite while a cam trough left a plain impulse unchanged. The wheels regularly moved one step after each cipher letter.

With this the decipherment of the cipher text had been accomplished. The reconstruction of the cam pattern of the wheels, which was set up new each day, was easily accomplished.

It should have been an easy matter to reconstruct the machine, to intercept the day's traffic on punched tape, by means of the tape to determine the daily setting of the wheels, to set up the corresponding pattern in the machine and then have the punched tape deciphered by the machine.

For the nine-channel cipher machine no receiving device was available which would unscramble the text. One piece of text which was unscrambled manually was not of sufficient length to permit any deductions as to the type of encipherment. It was certain that the cipher part differed in construction from that of the two-channel machine. Nevertheless in all of the cipher texts and between texts such parallel passages and repetitions were found that it is highly probable that a solution could have been reached had there been enough enciphered traffic.

Since the solution of the two-channel cipher device was very easy, due to a technical oversight which resulted in the machines idling while changing from transmission pause to plain text or cipher text, it was not necessary to make any study of the radio alphabet in connection with the Russian linguistic frequency curve in order in this way to find a method of solution, as was done in the case of the Siemens cipher teleprinter.

4. The English Cipher Machine.

The author had no chance to become acquainted with the English cipher machine and saw no report on it. Hence he can only say, based on hear-say, that it was very similar to the Enigma in construction but

instead of four wheels like the Enigma, has a set of five wheels of which the first does not change its position automatically when enciphering but is set by hand before each new encipherment. The function of the first wheel would therefore correspond in a certain way to the plug board of the army Enigma and would produce an initial alphabet varying from message to message.

A machine constructed like the Enigma but for enciphering ten digits instead of 26 letters is said to have been used by the Spanish Navy; it was never possible to get confirmation of this statement.

If even with manual systems any systematic character reduces the security of the system, this danger must be considered even greater in the case of cipher machines, since every machine encipherment is necessarily subject to certain regular characteristics and these regularities must be assumed to be known because of the rather wide distribution of the machines. The preceding studies of the various types of cipher machines have shown that the long period characteristic of almost all cipher machines does not guarantee security if the subperiods, of which the total period is composed, permit enough regularities to be recognized so that a solution of cryptograms is possible. Hence it is an inevitable requirement for any cipher machine which makes claim to security that all machine parts which affect encipherment shall be capable of different settings and that in addition the stepping of the machine shall be subject to marked irregularities which in their turn must also be influenced by different settings of the machine; furthermore the columnar substitutions(Spaltencäsar) should change their structure from column to column, in which connection an extremely high number of different alphabets is less significant than a high variability and the absence of recognizable systematic features in their structure. Unless these prerequisites are given adequate consideration, the security of cipher machines will be less than that of good manual systems.

SECTION C

THE SIGNIFICANCE OF INDICATOR GROUPS WITH CIPHER MACHINES

Whether it be because they are obtainable commercially, or because they are more widely distributed, or because their production cannot be kept secret as can that of a manual system, it is necessary for security reasons to make the assumption that a cipher machine as such is known to the unauthorized cryptanalyst, hence its entire claim to security lies in the fact that the immediate internal and external setting of the machine or the day and message keys are not known and cannot be recognized from the cipher text.

For this reason more attention must be given to the shaping of indicator groups for cipher machines than is required for manual systems. In general the daily key or the internal setting of the machine is arranged in advance so that the indicator's only function is to transmit the message key or the external machine setting.

But, since in many cases a knowledge of the significance of the message key is enough to enable one to match up the day's traffic in such fashion that it can be solved, it is necessary in any event that the message key or the indicator be transmitted only in enciphered form. In this connection the encipherment must be so handled that even a knowledge of all the indicators for a day will permit of no inferences as to their significance or as to the external machine setting. For this reason simple substitution tables cannot be regarded as adequate encipherment for indicator groups.

In many cases people have resorted successfully to preventing the actual message key from appearing even in enciphered form. Instead of this only a machine setting is transmitted in enciphered form, using which the encipherment of a pre-arranged text by the machine yields the message key; or a text is given which, when enciphered on the machine with a pre-arranged setting, yields the message key.

If cipher machines are used on a large scale one must also consider the danger which may result if unreliable operating personnel utilizes the choice of characters composing the indicator group to pass information regarding the internal setting of the machine, information which, when sent by radio, becomes

available to the unauthorized cryptanalyst. Hence in such cases regulations must be issued for the make-up of indicator groups or lists of indicator groups must be compiled which will limit or prevent misuse of these groups for other purposes.

Doc ID: 6592463

PART IV

GENERAL OBSERVATIONS

The point of this discussion of cryptographic systems was to show that the seemingly confusing multiplicity of systems can be reduced to very few simple basic concepts by a systematic arrangement. How small is actually the number of these basic concepts from which, in the long run, all cryptographic systems including the most modern hand or machine systems - can be derived - may be indicated by once more enumerating the concepts for basic systems which include among the substitution systems the simple substitution, digraphic substitution, polyalphabetic substitutions (Springcäsaren and Spaltencäsaren) as well as codes, and among the transposition systems the numerical key, grid and matrix transposition. With these all combined and reenciphered systems can be made up, if we add substitution tables and additive sequences as independent superencipherments.

With these few concepts we can embrace the entire field of cryptography. The field becomes difficult only through the number of possibilities which result in practice through combinations or through the different internal relations of the various systems.

The story is similar with the analysis of cryptographic systems on the basis of the cipher text available in a certain amount of traffic. Here again here are relatively few ways of making a count of the cipher text. An unknown cipher text can usually be dealt with by a chain count, displacement count, group count, frequency count or by a position count fully enough for the evaluation of the frequencies of the individual elements and/or parallel passages according to frequency, length, interval and position to permit an analysis of the system. The most time consuming of these counts, in cases where the cipher text shows no parallel passages, may be a position count, which may have to extend over all possible column widths and where the cipher elements often have to be torn apart both by columns and also by rows, corresponding to the number of cipher elements, until structural regularities

can be recognized which frequently consist in only slight deviations from an average determined by probability.

Here the art of the cryptanalyst consists in correctly estimating the significance of the clues derived from the various counts, clues which are usually few in number but may be of considerable extent, and in correctly judging them as a whole.

From the analyses of the cryptographic systems given in the examples it is quite clear that the concept of the security of a cryptographic system can only be a relative one, since it is very closely related to the amount of traffic enciphered with the system in question and available to the unauthorized cryptanalyst. Even the best cryptographic system possesses security against unauthorized decryption only within a certain amount of traffic, a limit which cannot be exceeded without endangering security.

In checking the security of a cryptographic system it is, therefore, necessary to ascertain first what the minimum amount of traffic is which will just make possible solution of the system. The answer can only be obtained with certainty by a thoroughly experienced cryptanalyst who has a complete survey of all the possibilities available in the technical field for unauthorized decryption and who can estimate their importance correctly. From this there follows necessarily below this minimum a maximum of traffic which may be enciphered with the system in question without endangering its security.

In determining this maximum, however, a factor of uncertainty must be included, the magnitude of which is determined by the following considerations:

1. The regulations governing the use of the system will not be followed exactly by the cipher personnel, as experience shows, as soon as unusual circumstances arise.
2. The greater the extent to which a system is used, the greater is the danger of possible loss or of compromise of part or all of the keys and other basic materials, due to some other causes.

Doc ID: 6592463

3. The repetition of an erroneously enciphered text, the encipherment of a similar text in the same system, the encipherment of the same text in two different key settings or in two different systems, the subsequent publication of parts of the secret text, etc. etc. represent dangers whose extent cannot always be predicted definitely and varies with the type of system.

Practical experience has shown that the factor of uncertainty, by which the previously ascertained maximum of traffic must be multiplied, is generally to be taken as at least one-half. According to the circumstances, a factor of uncertainty mounting to one-third or one-fourth may be recommended. In spite of all precautionary measures, a constant check on the observance of the rules laid down for a system and the amount of traffic to be enciphered in the system is very desirable because even the best cryptographic systems cannot be secure under all conditions when they are improperly used.